REVIEW
DIRECTORATE

DIRECTION GÉNÉRALE
DE L'EXAMEN

Fisheries and Oceans Canada
Pêches et Océans Canada

Canada

REVIEW OF THE MANAGEMENT OF INFORMATION TECHNOLOGY

APRIL 2000

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY 2

2.0 INTRODUCTION 8

2.1 BACKGROUND 8
2.2 OBJECTIVES AND SCOPE 9
2.3 METHODOLOGY 10

3.0 OBSERVATIONS 12

3.1 INFORMATION TECHNOLOGY IS ESSENTIAL 12
3.2 EXPENDITURES BY DFO ON INFORMATION TECHNOLOGY 13
3.2.1 Information Technology Expenditures 13
3.2.2 Expenditure Comparisons With Others 20
3.3 GOVERNANCE 24
3.3.1 Roles and Responsibilities 24
3.3.2 Need for Client-Provider Consultative Approaches 24
3.3.3 Large-Scale Systems 26
3.3.4 Administration of the IM/TS WAN 27
3.3.5 The Need for IT Support Outside Of Normal Working Hours 29
3.4 NEED FOR POLICIES 30
3.4.1 General Areas Where Improvement is Required 30
3.4.2 Want vs. Need 31
3.4.3 Evolution Of The Standard Office Suite 32
3.4.4 Internet – "Where Can I Go Today" 33
3.4.5 Access from Remote Locations 37
3.5 SECURITY 39
3.5.1 Threat and Risk Assessment 39
3.5.2 Physical Security of Assets and Information 42
3.5.3 Secure Authentication, Encryption and Public Key Infrastructure (PKI) 43
3.5.6 Security and Internet - Firewalls 43
3.6.7 Elimination of Single Points of Failure for Critical Systems 45
3.6 COMMUNICATIONS 45
3.6.1 Communication Channels 45
3.6.2 Web Publishing 46
3.7 TRAINING 47
3.7.1 Training Deficit 47

4.0 Recommendations 49

ACKNOWLEDGEMENTS AND THANKS 51

5.0. MANAGEMENT ACTION PLAN 51

1.0 EXECUTIVE SUMMARY

BACKGROUND

The presence of technology in the conduct of DFO's business is clear. The survey of departmental staff conducted as a part of this review in the summer of 1998 noted that 97% of staff have access to or use a computer in their day to day work.

Departmental Staff	%
Who have access to a computer in regular work activities	97
For whom information technology is necessary to deliver departmental responsibilities	81
For whom information technology is supportive of delivery of departmental responsibilities	69
For whom information technology is supportive of work with other departmental staff	72
Who use large scale custom designed applications	30
Who feel that their current system fully meets their needs	88
Who feel that their current system is sufficient for the next 12 months	74
Who have used the DFO Intranet in the past month	72
Who have used the Internet in the past month	82
Who use the Help Desk and find it good, very good or excellent	85
Who never call the Help Desk	24

The most valuable overall finding of this review is that DFO needs to manage information technology using clear business planning models that link current circumstances to future goals, include strong input from users, and clearly assess costs and technical implications.

Information Technology (IT) within DFO comprises all of the computer systems of the department, both hardware and software, and the networks linking them. Assets include over 8,000 personal computers as well as 18 large scale and custom software systems. These large systems do everything from providing a national recording system for fisheries violations to tracking the course of vessels at sea. A total of 94 computers are specially tasked as 'routers' to operate the WAN/LAN network. The technology enables employees of the department to carry out a host of functions including word processing, technical analyses, storing and transmitting data, doing research on the Internet, etc.

The focus of this review was to determine how well information technology was managed within DFO. The review, which was national in scope, addressed the following issues: the levels of capital and operating dollars spent on information technology; the management processes governing the planning and acquisition of information technology assets; the quality of service being provided; an analysis of recent patterns of IT utilization; security; and the use of the Internet.

It is important to note a number of key developments in managing information technology have taken place within the Department during this decade. In 1995, Corporate Services Information Management and Technology Services Directorate (IM/TS) began the task of developing a standard Informatics Architecture for DFO. They invited IM/TS staff and clients from all regions and NCR to participate. The architecture initiative has improved the technical efficiency of the networks and ensured that they can operate as an integrated whole. The architecture initiative included a comprehensive harmonization of hardware and software

SUMMARY OF FINDINGS

Spending on IT in DFO represents a significant component of overall expenditures. DFO's spending on IT in 1997-98 was $66.9 million dollars which is 6.1% of total departmental spending. Expenditures were allocated into six categories

Category	Expenditure (millions)	Per Cent of Total IT Expenditure
Hardware	$22.7	34%
Consulting Services	$19.6	29%
IM/TS Salaries (excluding library and central records)	$12.7	19%
Telecommunications (non voice)	$8.9	13%
Software	$2.9	4%
Supplies	$0.1	1%

This represents an annual expenditure per full time employee (FTE) of $6,658. This figure does not include the salary figures for staff in programs who spend all or a significant part of their time managing IT.

We also compared IT expenditures in DFO for 1997-98 with those in other government departments with like mandates. DFO spends more than either Health Canada ($5,400) or Agriculture Canada ($6,000) but less than Natural Resources Canada ($9,500) or Environment Canada ($9,700). In response to a request from Senior Management (made during the Departmental Review Committee's discussion of the interim report), we also made some more global comparisons with expenditures in North American business as well as U. S. governments at the federal, state and local level. These data showed large variations and that IT expenditures rise dramatically (16 fold) between organizations with a moderate commitment to IT solutions and those with more aggressive implementation.

DFO's overall IT expenditure of $6,658 per FTE breaks down to $2,818 (42%) by IM/TS and $3,840 (58%) within programs. In IM/TS, the largest expenditure is on salaries, followed by hardware, consultants, and data communications. High salary expenditures reflect the substantial body of in-house specialized expertise in IM/TS. In programs, where many of the large scale and custom software programs are developed, the largest expenditure is on consultants (42%). Given this large consultant expenditure, one could ask why IT managers in programs are not making

greater use of the in-house expertise residing within IM/TS. This is an area where significant cost savings could be realized. The reason it presently is not happening is due to the highly decentralized and uncoordinated decision-making process now in place for managing IT. Problems that are found in several sectors or regions have sometimes had specific, different and duplicative solutions developed. Roles, responsibilities and accountabilities need to be better defined. The following example illustrates this concern.

The department's current provider of telecom services has indicated that similar services are being purchased separately by the Coast Guard, and by IM/TS. They further indicated that savings could be achieved if all circuits and services were purchased in an integrated way. The review recommends that the Coast Guard, in cooperation with Corporate Services IM/TS and Public Works and Government Services Canada, Government Telecommunications and Informatics Services (GTIS), assess the degree to which cost savings can be achieved through harmonizing acquisition of these networking services. On a more general note, such duplication could be avoided if there were a clearer decision-making process to ensure that all IT investments are fully assessed, both for their support of program needs and for their compliance with departmental standards and architecture. We recommend that Senior Management define and clarify roles, responsibilities and accountabilities for the management of IT.

The last three years have seen several "one-off" investments in IT. Each of these has provided measurable benefits in line with the objectives of the investment. What has not been addressed is the provision of long term, stable funds, on an ongoing basis, to keep core activities operating and evolving in response to needs. Such a core functionality would likely include the WAN/LAN, operating systems, the desktop suite, help desk, and IT portfolio managers. It would be administered by IM/TS, both in Corporate Services and in the Regions.

Of all of the components in this core functionality, the network (including e-mail, the office desktop and user help) is the most important, mission critical component. Electronic mail, file sharing and integrated financial and personnel systems can occur only when the network is functioning properly. The review did a detailed topology of how the network operates and uncovered significant unevenness in its administration. A WAN is administered from the NCR, and several LANs are administered regionally as well as in the NCR. Each of these components is operated and administered in different ways in each region. Core funding has the advantage of eliminating this unevenness in administration and the level of service being provided to users. Also, we learned that significant cost savings could be realized if a consolidated, Department wide architecture for the WAN were created. Core funding would also eliminate the presently unevenly administered system of chargebacks for LAN management services in the NCR and some regions.

In order for the concept of a core functionality to work, there must be a clear definition of what is and is not included as well as an explicit and verifiable assessment of what level of funding should be provided. The review recommends that core funding be provided for the network, desktop, help desk and portfolio management components.

Clarifying accountabilities and core funding are necessary to strengthen the management of information technology. Such strengthening can only take place when the people responsible for IT management in IM/TS and programs make a greater effort to consult, learn and co-operate with each other. This includes a more concerted effort in consulting with and listening to users of information technology.

The concept of the 'portfolio manager' now used at NCR and in several regions is one approach that appears to work well in furthering consultation and cooperation. In this approach, IM/TS assigns an individual to become expert and provide continuity in meeting the IT needs of a specific program area. Where these positions exist and links to the program areas are nurtured, this is clearly a 'best practice'.

The status of consultation mechanisms between IT providers and users was examined as well. There currently are client/provider consultative mechanisms in various regions and sectors but no definable pattern exists. In the regions, we found some committees that had been struck for specific projects. Others were organized on a multi-sector basis or between one sector and IM/TS to address specific program needs. These were most apparent in Pacific where IT resources can easily be identified as resident in programs. At the national level, there was no client/provider committee structure at the time this review was conducted. In early 1999, a national Informatics Steering Committee (ISC) was formed. This committee is expected to become a key forum for taking action on many initiatives recommended in this review.

One example pointing out the need for a much more coordinated program of consultation is the rollout of Microsoft Office 97' desktop package now partially replacing Office 4.3. The review examined the management processes undertaken to justify the decision to upgrade the software and the degree to which users were consulted. The new version of the package was purchased as DFO's national standard even though a business case had not been developed showing the incremental benefits and despite inventory information which showed that a substantial number of users would be unable to move to the new standard. In addition, clients were not consulted on the need for the increased capability that Office 97' might bring. The cost of the Office 97 licence was estimated at about $700,000. However, the review determined that the introduction generated a training need that cost an estimated additional $900,000. The review recommends that future system- wide upgrades must be based on a full business case incorporating user input and must incorporate the cost of hardware upgrades and training. In addition, the review also recommends that Corporate Services IM/TS take the lead in developing a mechanism to address training needs that have been created by recent introductions of new software.

The review examined the degree to which the management of IT is presently conforming to standards and administrative policies. Such standards and policies most often pertain to questions of "who does what?" and "how are things done?". The existing lack of such policies and standards and the present degree of compliance or non-compliance with those standards, when they do exist, are illustrated by the following examples.

At present, DFO has a contract with the Government Telecommunication and Informatics Directorate (GTIS) of Public Works for the management of the IM/TS WAN. GTIS, in turn, has

contracted out the management of the system to a local firm, NUVO Networks. The review examined the detailed Services Level Agreement (SLA) which DFO has negotiated with GTIS. The review team found a lack of compliance in meeting the performance standards stipulated in the contract in the area of reporting and managing "bandwidth" (the level of traffic in the system). Also, GTIS, who is responsible for making architecture recommendations for the WAN; has not done so. Given the failure to perform to standards, the review recommends that Corporate Services IM/TS develop a comprehensive needs statement for the performance of the WAN. Remedial action should be taken if service levels are not met.

Another important area where the review team found there to be a serious failure in providing consistent service standards pertains to the management of the Internet. The departmental interface with the Internet is managed with six Internet "firewalls " throughout the NCR and regions. These are presently being managed inconsistently, without the benefit of a standard. The nature of the WAN/LAN is such that the least permissive firewall sets the risk for the entire system. The architecture of the electronic mail system was also identified as one with a high exposure to risk from the Internet. Given the present apparent vulnerability of the system, the review recommends that Corporate IM/TS conduct a threat and risk assessment on internet access and the configuration of the e mail systems to assess present levels of risk.

The review uncovered numerous other areas of inconsistency that could benefit from standards and consistent policies. The review recommends that Corporate Services IM/TS in Regions and NCR work with clients to establish reasonable and effective means for standardizing the following: firewall rules, levels of service, services that qualify for 24 hour support, services that must have no single point of failure, and service to remote locations, including ships.

A study of existing, large-scale systems was undertaken in the NCR and Maritime Regions to ascertain how they had been managed from conception to implementation. Large-scale systems were defined as costing over $500,000, delivered to more than 100 employees or implemented across multiple locations. At least two of the systems looked at in this review, the Departmental Violations Information System and the Habitat Referral Tracking System (HRTS), grew from an anticipated cost of less than $100,000 to an as delivered cost of over $1 million. The original estimate for HRTS did not reflect development, implementation or training costs, or the substantial costs associated with changing it from a WordPerfect based system to one based on Microsoft Word. Changes in the network operating system and the implementation of firewalls also caused the price of HRTS to increase to a final cost ten times greater than the initial estimate. Where detailed plans were absent costs were higher than anticipated and in some cases, deliverables did not appear in the year they were expected. Overall, it was found that systems that were developed through project specific teams that included staff from Corporate Services and Regional IM/TS as well as program experts and consultants tended to work best. Maritimes and Laurentian Regions have developed an effective planning system for large-scale systems. The review recommends that DFO ensure that all large-scale IT systems are assessed using a comprehensive project assessment and planning tool.

As part of its mandate, the review also addressed issues pertaining to present IT utilization and how this affects issues like the security of information, what constitutes "acceptable use " for DFO employees using the Internet and DFO communications.

The user survey revealed that of all of the shared IT services, it is electronic mail that is the most valued. The Coast Guard recently commissioned an extensive security study, which determined that the current e-mail system could be intercepted and tampered with. The review found no policy informing users of the security level of information that can be sent via e-mail. Therefore it is recommended that Corporate Services IM/TS notify users of the security level of DFO's current system and the types of information that can and cannot be transmitted

At present, all DFO users have access to the Internet. The average number of internet responses or "hits"per day (per full time employee) has been averaging about 28 at NCR, Maritimes, Newfoundland and Central and Arctic Regions. It has been averaging about 42 in Laurentian and 67 hits per day in Pacific Region. It was determined that about 10% of present DFO internet traffic is accessing subject matters with no apparent business purpose (including ads, news, business, sports and sex etc.). DFO has not monitored which Internet sites are being accessed. The review recommends that DFO provide an 'Acceptable Use Policy' to provide clarity on what is, and what is not acceptable for DFO employees using IT resources. An acceptable Use Policy was issued on May 28, 1999, while this report was being reviewed by DFO staff, prior to its release.

Finally, the review also briefly examined how IT has facilitated communications both within as well as with those outside of DFO. With respect to internal communication, the user survey provided some evidence of information 'overload'. There is no policy to indicate what types of information are appropriate for electronic distribution. The lack of clear policy direction is similar with respect to publishing on the Internet. The review identified that DFO spends about $2 million annually on Internet publishing. No mechanism exists to ensure that what is published is valuable and contributes to departmental objectives. Communications Directorate has the responsibility of enforcing departmental and Treasury Board standards but indicated they have not done any monitoring. The review recommends that Corporate Services IM/TS work together with Communications Directorate to ensure that an orderly and reasonable approach to the use of electronic communications is identified.

2.0 INTRODUCTION

2.1 BACKGROUND

Information technology is now an essential tool for staff in DFO in the delivery of departmental programs. This technology includes not only large and small computers but also electronic interconnection systems that link IT devices together. Computers themselves have evolved from research tools on room-sized mainframe computers and "typewriters with memory" into an interlinked infrastructure as indispensable as our buildings and telephones. According to the June 1998 telephone survey of the department conducted by PriceWaterhouseCoopers for this review, 97.8% of respondents reported that they use a computer in their *regular* work activities. Furthermore, 94% report that computers are essential to deliver their departmental responsibilities.

Originally, computers were simply stand-alone tools, used by specific individuals, programs and groups. As their use became more widespread, small groups became organized and tethered together in networks. At first, this was local "work groups", then larger and larger assemblages and now our current national system with continuous links to all but the most remote offices and ships (which are served through dial-up access, as well as cellular and satellite links).

Initially, the growth of DFO's architecture was within the department's work groups. Some, like Small Craft Harbours and Fish Inspection (which has since left the department), went so far as to establish a national stand-alone network; others implemented within-building links by "sector"; still others, particularly Science, began to work with colleagues inside and outside DFO using the Internet. The Coast Guard maintained inter-city electronic links directly and through Transport Canada to connect key offices across Canada long before merging with DFO. While steps have been taken to ensure that electronic mail and desktop applications in Coast Guard operate across the wide area network (WAN) managed by IM/TS, certain technical elements of the two systems remain very similar and are administered separately.

Following a suite of studies by Price Waterhouse of the department's Information Management/Technology Services (IM/TS) Directorate done between 1992 and 1994, as well as extensive work by IM/TS within DFO, a standard "architecture" emerged. Through the provision of targeted one-time funding, a more integrated uniform system was implemented. The DFO Informatics Architecture document and the subsequent infrastructure initiatives have dramatically improved the technical interoperability of the network and its systems. This process was effective in ensuring that the networks managed by IM/TS and Coast Guard could operate as an integrated whole. Issues remain, however, regarding planning, funding and managing the assets across the department so that they function effectively to support the department's needs in a cost-effective way.

While we are now physically linked together, the management of IT still differs widely across the department, even within one region or sector. Intersectoral tensions exist and problems that are found in several sectors or regions have sometimes had specific, different and duplicative

solutions developed without reference to the benefits that a higher level of coordination would have brought.

The management of IT is important as, over the past three fiscal years, DFO spent approximately $66.9 million per year (6.1% of overall spending) on IT (based on an analysis of spending by line object). This breaks down to about $6,658 per employee per year. While directly comparable data from other federal departments with a similar mission are not available, a comparison of non-salary expenditures has been conducted. Using these data, DFO's expenditures are in line with those of other similar Canadian federal departments (i.e. lower than Natural Resources and Environment while higher than Agriculture and Agri-Food, and Health). A table of these expenditures can be found in section 3.2.2 of this report.

2.2 OBJECTIVES AND SCOPE

The management of IT was assessed from the following perspectives:

- a general assessment of operating and capital dollars and FTE's directly involved in the management of IT
- the implementation of an appropriate interface for policy and planning among all managers of IT across the department, and between these managers and their respective clients
- the nature and effectiveness of the strategic planning tools in use in all parts of DFO that govern the acquisition and management of IT
- the department's ability to support and promote the use of technology to sustain and improve:
    1. program delivery to clients
    2. staff productivity
    3. communications within the department
    4. provision of information on program results and financial status to managers
- compliance with Treasury Board policy

A sample of recent investments was assessed to determine if they were evaluated and implemented within an information management framework. The examples for review were drawn from large scale systems found in all relevant sectors. Recent investments in hardware, software, and services include: Abacus, Peoplesoft, Windows NT server, Office 97 upgrade, Microsoft Exchange/Outlook, the Habitat Referrals Tracking System, the Departmental Violations system and the implementation of a new desktop hardware standard. A summary analysis of the strategies and consultation that preceded these acquisitions was made. It was important to identify where projections regarding cost savings and other benefits such as decreased downtime and increased reliability were made prior to implementation of these system changes, as well as the attainment of the anticipated benefits.

The scope of this review included the management of hardware, custom and commercial software, interlinking and network communicating tools, fixed installations and portable hardware. Also included was IT that is provided to the department on a lease, rental or license

basis (excluding local and long distance voice telephone). As a key part of this review the delivery and support mechanisms were identified and assessed.

This review coordinated its work with the Review of Corporate Services Redesign and the Governance Options Project, and took into account all relevant inventory work that has already been completed. As well, information from recent studies that bear on the management of IT (e.g. Peoplesoft, Abacus) was utilized where appropriate.

2.3 METHODOLOGY

The review was conducted from February to December 1998. Specific studies were conducted, some by staff in DFO's Review Directorate and some by consultants under their direction. Significant efforts were made to work closely with key departmental personnel as the review moved forward.

There were three major and five minor lines of enquiry. Only one of these, the user survey, will be released as a separate report. In addition to these lines of enquiry, every major DFO study of IT, networks, the informatics function and IT security conducted since 1991 was assessed for its currency and relevance to the objectives of the study.

The three major components were the user survey, the analysis and benchmarking of department-wide expenditures on IT and a review of the WAN, Internet and security.

1) The user survey of departmental staff was conducted by telephone in the summer of 1998. It presents results by region and by sector with 90% accuracy. The survey results were compared to similar surveys conducted in other organizations. Areas of key achievement (best practices) and areas requiring attention were identified.

2) Departmental expenditures covering the three most recent fiscal years (1995-96, 1996-97 and 1997-98) were analyzed and benchmarked. IT-related objects of expenditure were identified and mapped across the systems in old DFO and in the Coast Guard through the three-year period. All expenditures in the department were sorted by region and by sector, with old DFO being reported by business line and the Coast Guard being reported by responsibility centre. The expenditures were graphed and trended, with inter-region and inter-sector comparisons being made. The figures were then benchmarked against Full-Time Equivalents (FTEs) (as found in the Salary Management System) and against total expenditures (by region, by sector and nationally). The most important analysis was to look at inter-region, inter-sector and inter-year comparisons. Department-wide expenditures were then compared against expenditures made by the three other "natural resource" departments and Health Canada. Broader benchmarking against North American business and U.S. federal, state and local governments was also done. Although these are somewhat remote from DFO's situation, they help to determine if the department is in line in a larger context and were requested by senior management during an interim reporting meeting.

3) The third major study was conducted on the "backbone" components of the network. This included the WAN connecting all major departmental centres, its capacity and the utilization of that capacity as measured by daily reports commissioned by the department. The study also looked at patterns in Internet traffic at each of the department's six "firewalls" (devices that interface between DFO's network and the Internet). The purpose of this component was to assess the volume and nature of Internet use and the degree to which this is a cost factor for the department's infrastructure. The final component of the study was an assessment of security issues. This component focused on the implementation of reasonable and necessary security measures regarding protected information, physical security of Local Area Network (LAN) and WAN devices, and security against unauthorized access from any source (including the Internet).

The five minor components were:

1) an analysis of departmental IT management policies, committee structures, and planning documents to assess their scope and efficacy, as well as the degree to which they relate to DFO program needs and incorporate client input;

2) an analysis of the management of departmental large-scale custom software systems which operate at either a national or at a regional level to assess the business case that was made, as well as the procurement and development processes used and the degree to which the product met the initial objectives and cost estimates;

3) an analysis of current management practices and policies surrounding remote access to DFO computer systems to assess compliance with policies, costs and the degree to which DFO has implemented teleworking opportunities;

4) an analysis of the management processes used to decide on a recent change to the standard departmental office suite (from Microsoft Office 4.3 to Microsoft Office 97) that affected every user in the department. This was done in order to identify what implicit and explicit management processes were used to identify the business requirement, and the specific product, as well as the degree to which the users were a part of the decision making process, and what business related improvements have been delivered to departmental users as a result of this change; and

5) an analysis of the management of Web publishing on both the Internet and the internal government-wide Intranet to determine the degree to which this new communications channel has been subject to the same standards, constraints and considerations as printed publications, as well as to assess the costs and, where possible, the effectiveness.

3.0 OBSERVATIONS

3.1 INFORMATION TECHNOLOGY IS ESSENTIAL

Given the long history that DFO scientists have had using computers, as well as early use of proprietary systems for such office functions as Ministerial correspondence, reviews and assessments of the department's use of IT are as old as the technology itself. Only the most recent IT related studies since 1991 were looked at as a part of this review. In virtually all of these recent studies there has been a consistent call for a higher level of organization and integration in the use of computers and the achievement of a greater level of support for the department's programs from what is now generally called IT.

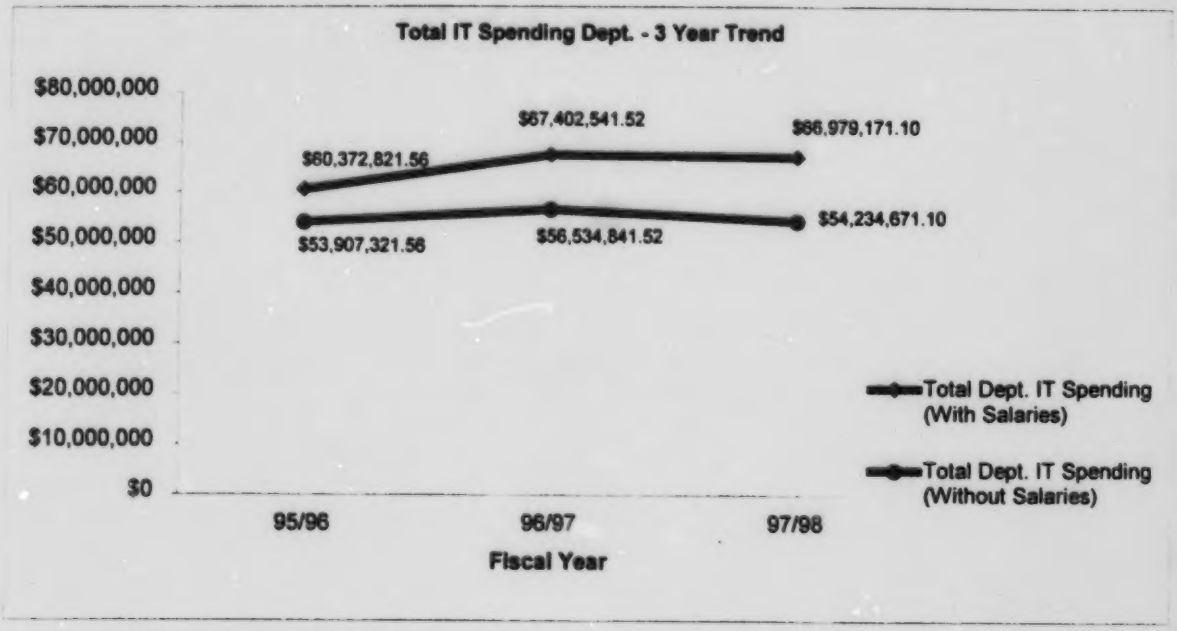
While departmental spending on IT occurs in every region and sector, 56% of the 1997-98 IT spending was in Corporate Services (42% of the department's spending was in the IM/TS component of Corporate Services.) The sector with the next highest level of spending was Coast Guard which spent 25% of the departmental total. This review looked at spending in all sectors and regions, but more closely at IM/TS spending. This reflects not only the highest area of spending but also the group with the core responsibilities for managing IT related matters in DFO. The other areas in Corporate Services with high IT spending, Abacus and Peoplesoft, have already been subject to detailed review and have not received detailed assessment in this review.

The networking of computers (that can share files and e-mail that are compatible) is the most important "value added" to the department as a whole. While individual machines operating specialized systems can be mission-critical for specific program components or even entire programs, the communications advantages of the network working as a whole make the network possibly the most mission-critical IT asset in the department. The network, in the various studies that underpin this report, is clearly essential to program delivery. Electronic mail (e-mail), file sharing and integrated financial and personnel systems can occur only when the network is functioning properly. It is as essential and as basic as the buildings in which we work and the vehicles that we use to deliver our programs.

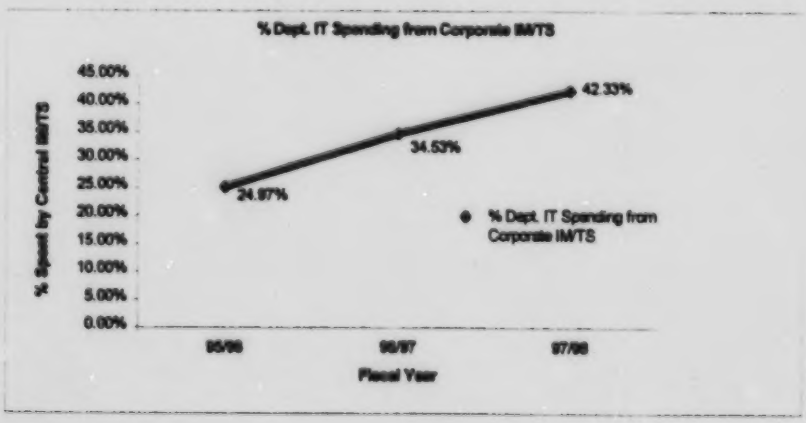
The review found significant unevenness in the administration of the network, service levels and chargebacks, user support, the involvement of clients and the implementation of the standard office suite. The standard office suite and e-mail comprise the two national software standards that support communication among all parts of DFO. E-mail is well integrated and generally functions in an orderly and reliable way. A WAN is administered from the National Capital Region (NCR) and several LANs are administered regionally (as well as in the NCR). Each of these components is operated and administered in different ways in each region. In some regions, there is core funding for IM/TS and, in others, there are chargebacks which vary widely in the amount and scope of services which are linked to the chargeback.

3.2 EXPENDITURES BY DFO ON INFORMATION TECHNOLOGY

3.2.1 Information Technology Expenditures



An analysis of all departmental expenditures on IT was conducted for 1995-96, 1996-97 and 1997-98. Although these years include the first year of the DFO-Coast Guard merger and several cases of one-time funding in various areas, the expenditure patterns are quite stable.



Over the three years, while the departmental total has remained fairly stable, the amount that is expended through IM/TS has grown from 25% to 42%. This reflects in part special "infrastructure" spending in 1997-98 and also the expansion of "service level agreements" which transfer funds from programs to IM/TS.

The department's IT expenditures on a per FTE basis are shown below.

Exhibit 3.2.1.1 Departmental IT Expenditures Per FTE (1997-98)

Component	Expenditures
All of DFO	$6,658
Spent Outside IM/TS	$3,840
Spent by IM/TS	$2,818

Exhibit 3.2.1.2 1997-98 IM/TS Chargebacks Per Region

Region	Chargeback Per FTE
Newfoundland	$0
Maritimes	$1,050
Laurentian	$0
NCR	$1,000
Central and Arctic	$0
Pacific	$0

The two tables above, when taken together, confirm that the chargeback system for IT services is uneven and that the amount charged back bears no evident relationship to actual expenditures by the IM/TS groups in individual regions or the NCR.

Exhibit 3.2.1.3 Analysis of 1997-98 IT Expenditures Per Departmental FTE

Expenditure Type	IM/TS Expenditures Including Salary	IM/TS Expenditures (non Salary)	Program Expenditures (non Salary)
Expenditures per FTE	$2,818	$1551	$3,840
Salaries	45%[1]	0%	0%[2]
Hardware	28%	51%	38%
Consulting Services	12%	22%	42%
Data Communications	11%	20%	15%
Software	4%	7%	5%
Supplies	<1%	<1%	<1%

[1] Throughout the report IM/TS expenditures on Libraries and Central Records have been removed where information about expenditures provides for such a determination. Data are from DFO's Financial Management Reporting System, Abacus and the Salary Management System.

[2] This study did not attribute program salary dollars to IT activities. The analysis instead is of expenditures by line object, which is the most readily verifiable information. A larger A-Base type review would be required in order to accurately determine salary expenditures directly attributable to the management of IT.

This table, based on line object groupings, demonstrates that the amount spent within programs ($3,840) is similar to the amount spent by IM/TS ($2,818), although the products and services are very different. Even though IM/TS retains consultants for such functions as Help Desk, their largest expenditure is on salaries, followed by hardware, consultants and data communications respectively. This contrasts sharply with the profile in programs. Here, where many of the large scale and custom software is implemented, 42% of the spending is on consulting services. The IM/TS salary figure confirms that there is significant expertise within the department. It is possible that more effective use of this experience could reduce the need for programs to spend on consulting services. It is also important to note that the expenditures on data communications are of a similar magnitude in programs (15%) and IM/TS (20%). While some data communications are charged back, this suggests that programs are operating data communications systems entirely within program areas. Given the funding pressures within DFO at this time, there would appear to be an opportunity for savings if some of these data communications systems were consolidated. Anecdotal discussions with the Government Telecommunications and Informatics Services component of Public Works and Government Services Canada (GTIS), which supplies WAN services to Corporate Services and digital circuits to the Coast Guard, indicate that even harmonizing the acquisition of services would lead to savings, and that further integrating the management of these two systems could lead to even greater savings. While the Coast Guard inter-city links, which are used for navigation-related information (including digitized voice communications), needs a high level of reliability, as GTIS is the supplier to both, it would seem that harmonization of the management of these similar systems within DFO should be assessed.

Exhibit 3.2.1.4 Analysis of 1997-98 IT Expenditures Per FTE By Programs and IM/TS By Region

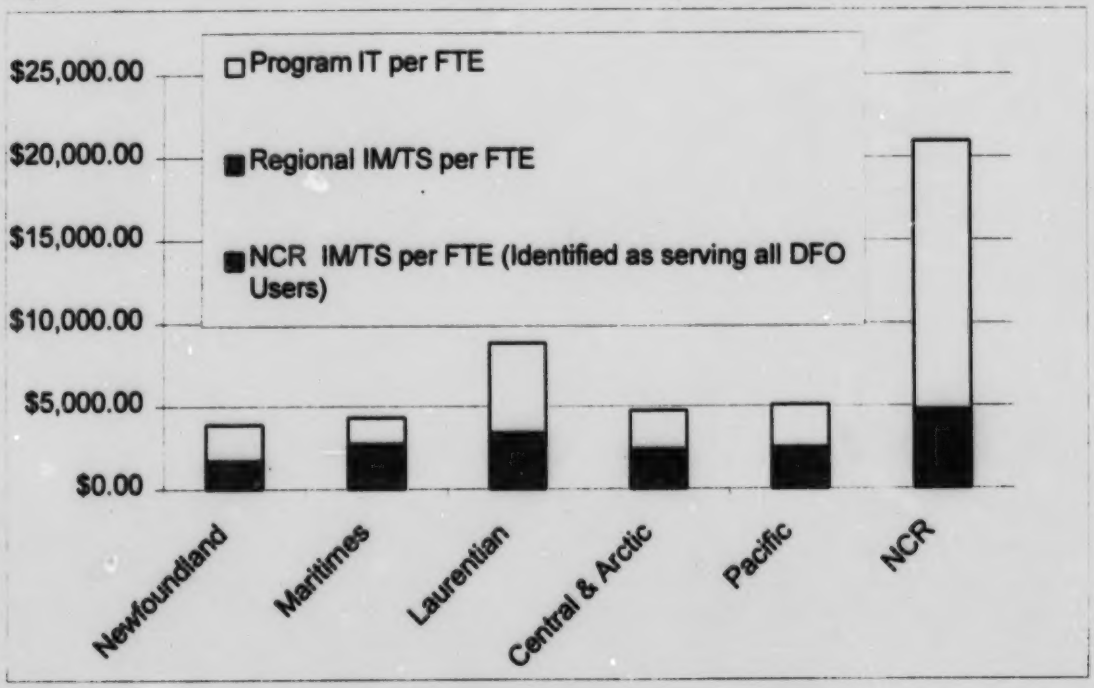


Exhibit 3.2.1.5 1997-98 IT Spending Per FTE Per Region

Region	NCR IM/TS Spending Identified as Serving All DFO Users	Expenditures By Regional IM/TS	Expenditures By Programs on IT	Regional IM/TS Spending as Percentage of Program Spending on IT in that Region
Newfoundland	$748	$938	$2,200	43%
Maritimes	$748	$1,976	$1,611	123%[3]
Laurentian	$748	$2,649[4]	$5,419[5]	49%
Central and Arctic	$748	$1,638	$2,352	70%
Pacific	$748	$1,740	$2,558	68%
NCR[6]	$748	$4,017	$16,210	25%
Average Cost Per FTE Across DFO in 1997-98: $6,658				

The foregoing table shows that delivery models vary widely from region to region. Even the direct expenditures (including salaries) of IM/TS in each region vary from 25% of IT expenditures by programs in the NCR to 123% of the expenditures by programs in Maritimes. The situation in Maritimes reflects the significant transfer of program monies into IM/TS for expenditures under service level agreements. While IT expenditures in the NCR are the highest (four times that of Newfoundland), the NCR is also where many national program systems are developed and operated. These systems (e.g., the Departmental Violations System, the Habitat Referrals Tracking System and others) bring workload that is unique to the NCR, with the exception of the Coast Guard INNAV system which is being developed in the Laurentian Region for application in the East Coast. When IM/TS costs are shown as a percentage of these national systems, the NCR (even with the highest overall expenditures per FTE) comprises the smallest component.

Providing an adequate level of funding to the network and related elements in all regions as well as to the WAN (which is administered in the NCR for the entire department) is appropriate given the essential nature of the networking function. One way of providing the necessary funds could be that funds would be provided directly from the department's base at an early stage in the budgeting process. It is important to note that the portion of the department's IT expenditures attributed to the WAN managed by IM/TS is very small (just over 10% of all IT spending in DFO) when compared to other costs, notwithstanding the critical support this WAN provides to departmental activities.

[3] Under service level agreements, over $5 million is transferred from programs for expenditure by IM/TS.
[4] Laurentian Region has reported that they began large scale year 2000 related spending in 1997-98 which may contribute to this higher figure.
[5] This large expenditure includes two specific components. The Laurentian Region initiated large scale year 2000 projects in 1997-98. Further , the Coast Guard INNAV system, a multi-million dollar custom system for the Atlantic that is being developed in the Laurentian Region, is a significant and anomalous component that pushes up program spending per FTE.
[6] In this analysis, the NCR is treated like a region, NCR IM/TS reported an expenditure level that they identify as benefiting all users in DFO.

In those regions where IM/TS has instituted chargebacks, considerable effort is expended in identifying what is charged back for the network and related elements. A measurable effort is also spent in chasing "bad debts" where programs fail to provide the agreed-upon fees, especially where some services (like the WAN) cannot reasonably be removed to force payment. More consistent approaches (on a per FTE basis) would seem to be possible given the wide variation shown above.

Exhibit 3.2.1.6 1997-98 IT Expenditures Per Sectoral FTE By Sector

Sector (All Regions)	Per Sectoral FTE Expenditure
Corporate Services	$27,385[7]
Policy	$5,605[8]
Science (including Oceans)	$3,680
Coast Guard	$3,513
Fisheries Management	$2,903
Average Cost Per FTE Across All DFO in 1997-98: $6,658	

The above analysis shows that with the exception of Corporate Services, which houses not only the IM/TS function but also Abacus and Peoplesoft, the program expenditures per FTE on IT are on the same scale. This is especially noteworthy as Science is often considered as a "large-scale user" of IT; however, on a per FTE expenditure basis, it is in line with the Coast Guard and similar to Fisheries Management. It is important to note that, given the support role that Corporate Services has for the department, the "per Corporate Services FTE" figure cannot easily be compared with expenditures in other sectors, but has been included for completeness.

The last three years in DFO have seen several "one-off" investments in IT. Each of these has provided measurable benefits in line with the objectives of the investment. What has not been addressed is the provision of sufficient funds, on an ongoing basis, to keep these core activities operating and evolving in response to needs. These "one-off" investments (such as the Common E-mail and Infrastructure project) can solve specific "catch up" problems: however, these sorts of urgent catch up/rust out expenditures can be avoided through a recognition of the need for ongoing maintenance of the core functionality. This core functionality can be derived through the client/provider business line consultations recommended elsewhere in this report, but would likely include the WAN/LAN, operating systems, the desktop suite, help desk and IT portfolio managers, and the necessary needs based evolution of these systems.

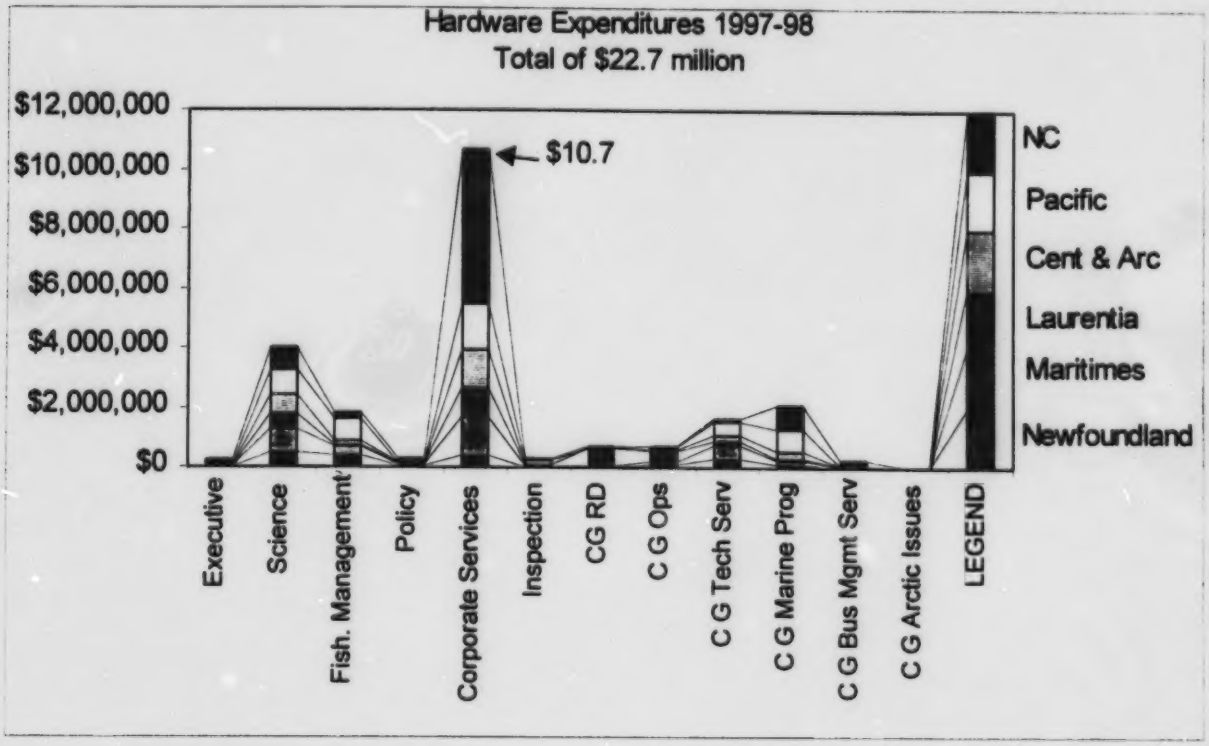
The department's expenditures fall into four large line object groupings. A comparison of the spending patterns between DFO and other departments with similar missions follows. The spending patterns, when presented by line object groupings, by sector (and business line in Coast Guard) by Region help to identify how IT management strategies differ. The information is presented by line object grouping, as follows: hardware, software, consulting and data

[7] This includes not only IM/TS support for the department but also Abacus and Peoplesoft and others, which are also support for all program areas.

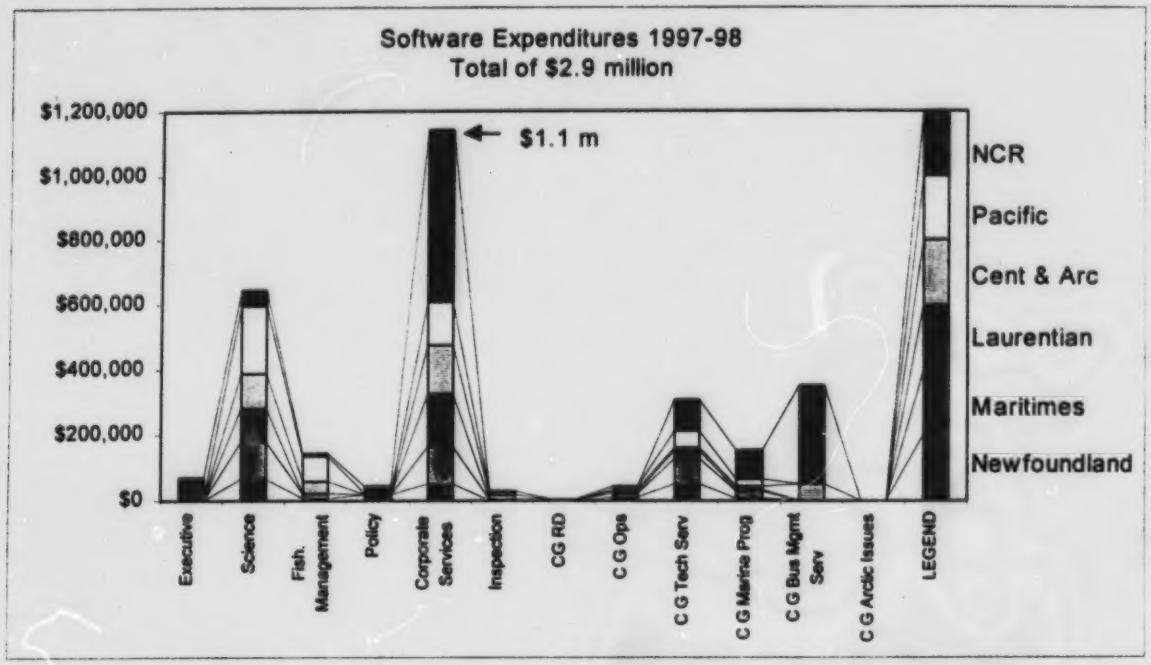
[8] The two largest components of this are consultants in Maritimes ($320,000) and hardware in the NCR ($160,000)

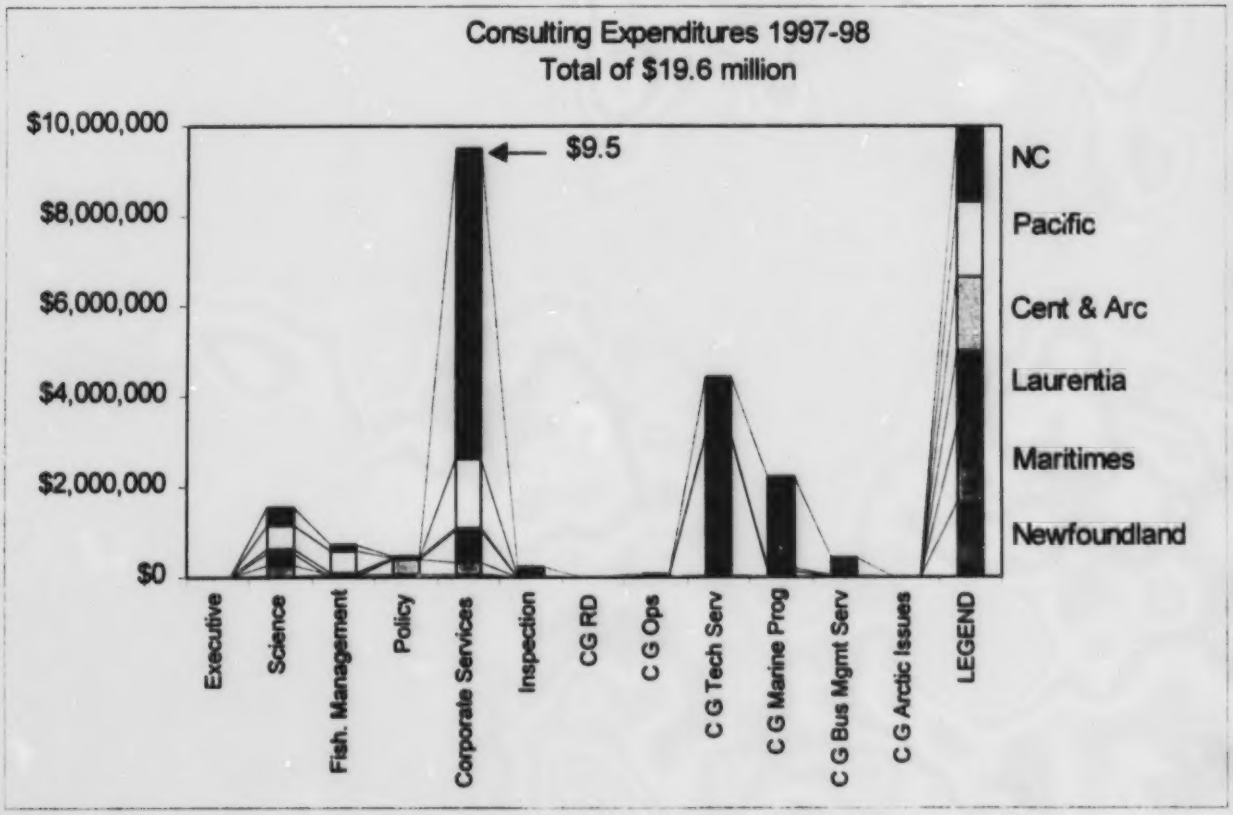
communications. The sectoral and business line categories represent individual bars, and the region where the spending took place is represented by a consistent marking scheme. As the graphs change in scale the value of the highest bar is identified on each graph

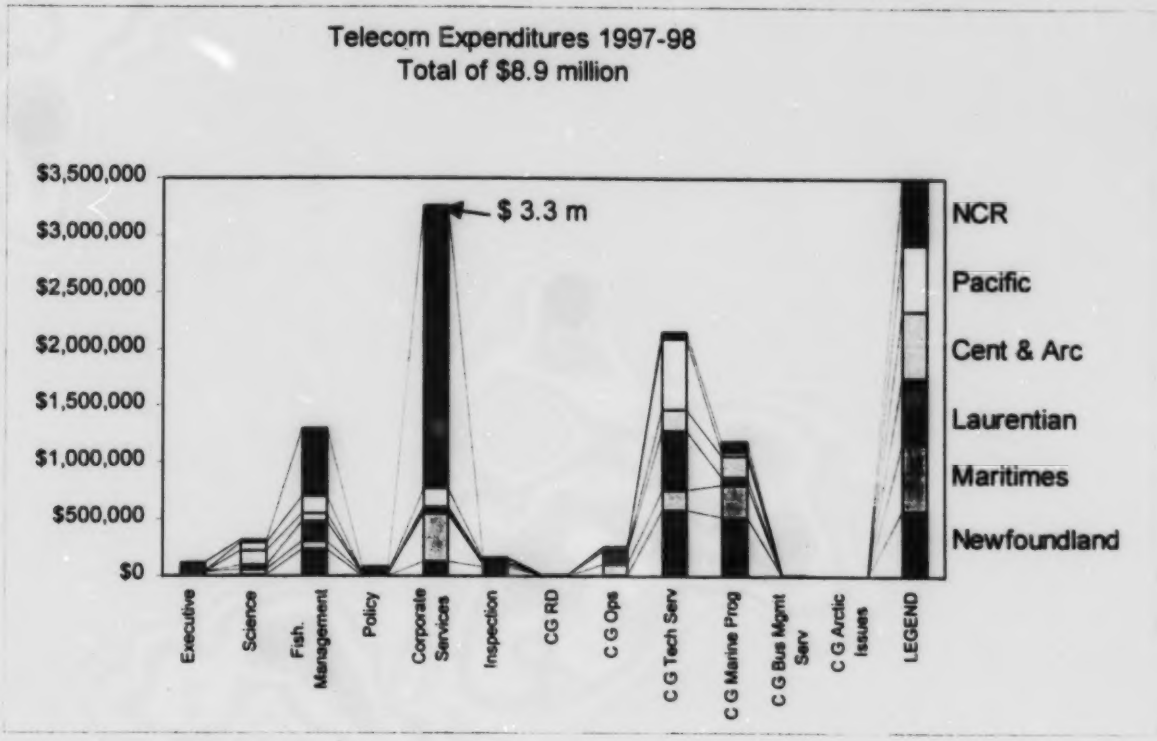
Exhibit 3.2.1.7 1997-98 IT Expenditures By Line Object Grouping By Region and Sector or Business Line[9]



[9] The Fish Inspection group appears in these graphs, as it does throughout the report as it was a component of the department during the three fiscal years analysed for this review. Its inclusion allows for the verification of results against consolidated departmental reports which include all sectors and regions.


Software Expenditures 1997-98
Total of $2.9 million
$1,200,000
$1,000,000
$800,000
$600,000
$400,000
$200,000
$0
$1.1 m
NCR
Pacific
Cent & Arc
Laurentian
Maritimes
Newfoundland
Executive
Science
Fish. Management
Policy
Corporate Services
Inspection
CG RD
C G Ops
C G Tech Serv
C G Marine Prog
C G Bus Mgmt Serv
C G Arctic Issues
LEGEND


Consulting Expenditures 1997-98
Total of $19.6 million
$10,000,000
$8,000,000
$6,000,000
$4,000,000
$2,000,000
$0
$9.5
NC
Pacific
Cent & Arc
Laurentia
Maritimes
Newfoundland
Executive
Science
Fish. Management
Policy
Corporate Services
Inspection
CG RD
C G Ops
C G Tech Serv
C G Marine Prog
C G Bus Mgmt Serv
C G Arctic Issues
LEGEND



3.2.2 Expenditure Comparisons With Others

Expenditure data (by line objects) from all federal departments and agencies were analyzed. While each department is different, the expenditures of the three other "natural resource" departments (Environment, Natural Resources, and Agriculture and Agri-Food) and Health Canada were chosen as sufficiently similar to merit comparison.

All departmental expenditures were "benchmarked" as costs per FTE and as a percentage of the overall budget (less grants and contributions). As noted, DFO's costs in this example are derived from the same tables as the other departments and therefore do not include expenditures (such as IM/TS salaries) that are included in all other parts of the review.

Exhibit 3.2.2.1 1997-98 IT Expenditures in Related Departments

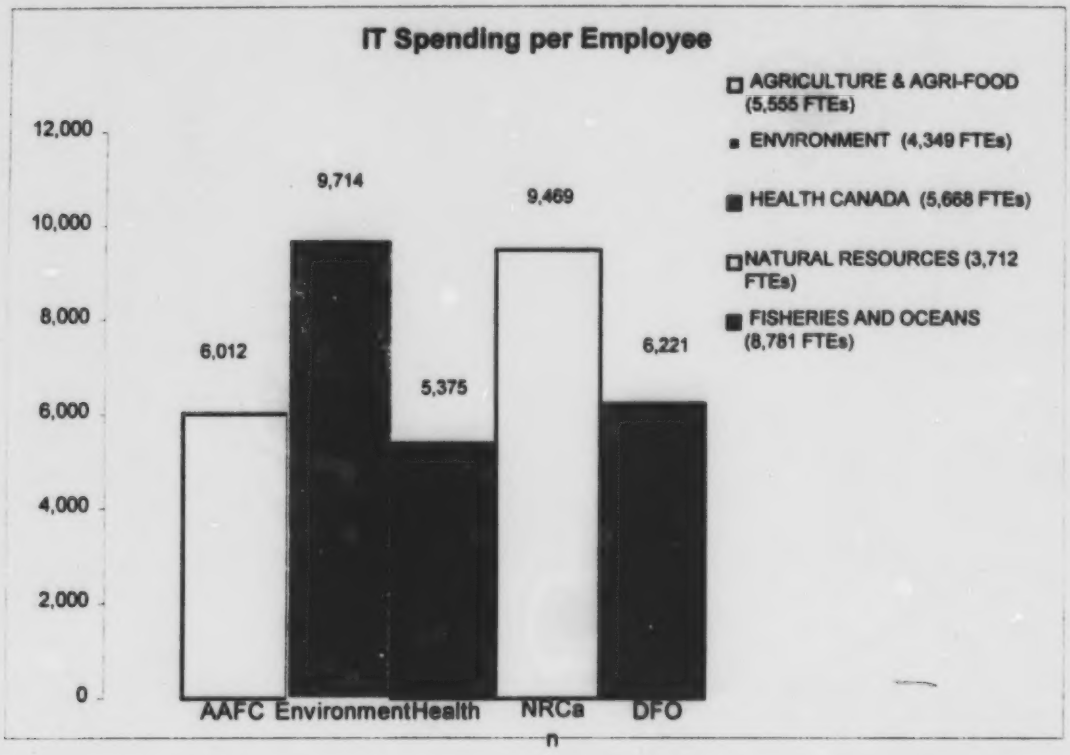
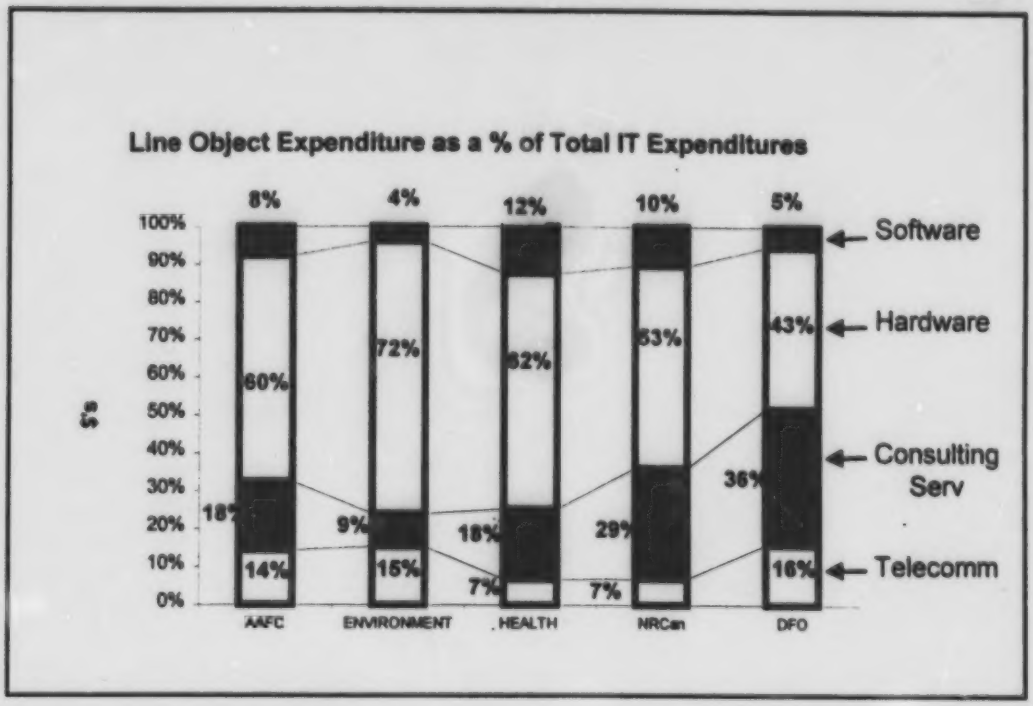


Exhibit 3.2.2.2 1997-98 IT Expenditures in Related Departments As A Per Cent of Base

Department	Per FTE Spending	Per Cent of Base
Health Canada	$5,375	2%
Agriculture and Agri-Food	$6,012	2%
DFO (TBS figure)[9]	$6,221[9]	4.8%[10]
Natural Resources Canada	$9,469	7%
Environment	$9,714	7.6%

[10] The Treasury Board Secretariat figures do not include salaries for DFO or for any other department, and this explains the difference between the DFO figure shown here and the overall expenditure per DFO FTE figure of $6,658 for DFO used in all other places in this report.

Exhibit 3.2.2.3 1997-98 IT Expenditures in Related Departments By Line Object Group



The foregoing analysis of expenditures showing percentage of total IT expenditures by line object groupings shows that there is significant variation in the manner in which IT monies are spent between the five departments. While DFO has the lowest spending on hardware, it spends more, on a percentage basis, than any of these other departments on consultants.

The following table shows "per FTE" expenditures for North American business, as well as governments at the federal, local and state governments in the United States. This table has been included as, during the discussion of the interim report at the Departmental Review Committee, a request was made to situate DFO's expenditures in a broader context, including the private sector. It is useful to note that notwithstanding the many weaknesses of this type of global comparison, DFO's spending per employee is on the same scale as that of business across North America. The table also shows that IT expenditures are heavily skewed and that while 50% of companies spend less than $7,000 per employee, this jumps to over $24,000 when 75% of the companies are added. This presumably reflects the level of reliance on IT for business purposes. The value of that information is to indicate that for those organizations that rely heavily on technology, costs per FTE can rise to a very high level. This is most apparent in the U.S. federal government where 50% spend less than $1,500 while 75% spend over $25,000, even more than comparable business expenditures. These global comparisons hold less value for DFO than the foregoing assessment of like Canadian federal departments, other than the observation that IT expenditures can rise dramatically (16 fold) between organizations with a moderate commitment to IT solutions and those with more aggressive implementations.

Exhibit 3.2.2.4 1997-98 IT Expenditures ($Can) in Government and Industry

Organization	25% spend less than this per employee	50% spend less than this per employee	75% spend less than this per employee	50% spend this per cent of overall expenditures
North American Business	$2,208	$6,996	$24,012	2.9%
U.S. State and Local Governments	$3,585	$11,481	$35,881	0.8%
U.S. Federal Government Departments	$810	$1,472	$25,636	1.7%
DFO actual spending is $6,658 per employee, which is 6.5% of total spending.				

The analysis of the Canadian Federal departments shows that IT represents a significant portion of departmental spending and is generally in line with the expenditures of the other federal natural resource departments. Projections of these expenditures into the future are difficult as there is a material difference in cost between a "stand pat" needs-based model and one which commits to aggressive implementation of IT in new areas. This report examines, among other things, how these expenditures are made across the department and the degree to which changes would be beneficial in terms of performance and value.

The most powerful way to eliminate duplication and inefficiencies is to consult, co-operate and consolidate with a view to achieving consistency. While there are organizations and approaches that can dramatically reduce costs (e.g., a high degree of central control, a short list of approved hardware and software), it is not clear that DFO's program needs and management traditions would support this approach. The strategy with the greatest probability of success is one in which there is genuine cooperation between clients and providers, as well as an appreciation of the benefits of consolidation. This model was found to exist, usually for specific projects or initiatives in Maritimes, Laurentian and Pacific Regions, and the NCR.

The department will realize tangible benefits from treating the network (including e-mail, an office "desktop" and user help) as a departmental asset. For this to be effective, this specialist group (IM/TS) needs to receive adequate funding not only to operate but also to maintain and evolve this activity. In several regions, there is a management model where "portfolio managers" are assigned by IM/TS to become experts in the needs of a particular business line. Where these positions existed, and links to the program areas were good, this was a "best practice" that did much to bring cooperation and consistency.

A key recommendation of the review can also be found in the 1994 Price Waterhouse report on IM/TS; specifically, "...end the practice of user chargeback for LAN management services. These services should be corporately funded." In order for this to occur, there must be a clear definition of what is and is not included, as well as an explicit and verifiable assessment of what level of funding should be provided. This recommendation is still a good one and its implementation would

do much to address problems of inconsistency, inadequate levels of service in some areas and the time and effort made chasing chargebacks. In order for this to occur, there must be a clear definition of what is and is not included as well as an assessment (possibly by the committee structure proposed in the "Recommendations" section of this report) of what level of funding should be provided.

The level of funding cannot be clearly set without agreement on whether to pursue a strategy of adequate support to program goals, or one in which DFO is on, or close to, the leading edge of the implementation of IT. There are substantial differences in the levels of risk and expenditures between being an efficient manager of IT and being on the "leading edge".

3.3 GOVERNANCE

3.3.1 Roles and Responsibilities

A key general finding, which occurred across all lines of enquiry, was an absence of effective implementation of relevant and meaningful policy. In some cases, this is an absence of a policy of any kind, while in others it is the absence of implementation of existing policies. The "who does what" and "how are things done" types of policy are the most important here.

The lack of such policies (lack of implementing of those that do exist) have resulted in a patchwork of approaches. This weakness has the largest impact on DFO's business in the area of custom and large-scale systems. The next most serious weakness is in the area of hardware and software acquisition. Another area where there is an absence of consistency is those services for which IM/TS is responsible in different regions. The presence or absence and level of chargebacks to programs is also inconsistent. Some regions keep high levels of IT expertise in program areas (e.g. Pacific), while others (e.g. Maritimes) have consciously moved staff from programs into IM/TS. There is even a middle ground (e.g. Laurentian) where some staff are funded by Science and are managed by Corporate Services. A number of important areas are identified in the report that will benefit from a higher level of consistency. This can be achieved through greater cooperation and consultation between program staff and staff in IM/TS. This cooperation, to provide all the benefits that are available, must be accompanied by clear agreements on where regional IM/TS and program coordinating committees can make binding recommendations governing expenditures and where their role is simply that of advisor.

3.3.2 Need for Client-Provider Consultative Approaches

In the 1993 and 1994 Price Waterhouse reports, there was a call for client-provider committees that would facilitate the use of IT. This requirement remains today. In any successful service relationship, the needs of the client must be the guiding force for the services rendered. There are two tiers: services that are provided without charge; and cost-recovered services. In discussions on the first tier, it is important for a mechanism to exist to ensure that requests are truly in line with needs. This mechanism could be that the evolution of core-funded services must be approved by all sectors, since sectors may need to accept lower levels of overall funding if new levels of service or services are deemed to be "core".

There currently are client-provider consultative mechanisms in various regions and sectors, but no definable pattern exists. At the regional level, we found some committees that had been struck for specific special projects. In a very few cases, region-wide multi-sector committees had been formed and in some cases members saw them as working well. There were also committees in which one sector would work with IM/TS on specific program needs. These were most apparent in Pacific, where IT resources can easily be identified as resident in programs.

At the national level, there was no client-provider committee structure during the period of the review. A committee made up of directors of IM/TS periodically invites those at lower levels in IM/TS, but these larger meetings occur only once or twice per year. A national client-provider committee (called the Departmental Informatics Working Committee) has not met for over a year, and appears to have been dissolved. In early 1999 the department established the Informatics Steering Committee (ISC) representing all parts of DFO. This committee will act as a steering committee for IT related matters. This is a beneficial step that can be the basis for resolution of several key issues identified in this review.

There is a clear need for at least two levels of national client/provider discussions. The first would be a high level forum with some of the responsibilities that have been proposed for the new ISC. This high level committee, to be effective, needs to be supported by other structures that are more able to address detailed and sector or region specific issues. These other structures/committees could consider how the department should address emerging uses that place significant new demands on the WAN/LAN than simple e-mail and text sharing. There are several cases now (including INNAV and multimedia) which, if implemented, would have the ability to stress the network's current capacity. The committees and working groups that support the ISC could focus on long-term strategic uses of IT. These uses are almost limitless, and there is a need to link program needs and desires with cost factors, technical feasibility and desirability. Given the costs and complexity associated with large scale use of IT based solutions (as shown in the expenditure data in the previous section demonstrating a rapid rise in expenditures between average, and above average organizations) it is important that "pilot projects" are well-designed and the results are widely shared. This is done on a very small scale now by a few sectors, but there is no large-scale sharing of experiences and ideas.

DFO could also benefit significantly from a user-provider updating of the informatics architecture standard. The creation of the DFO Informatics Architecture document and the subsequent infrastructure initiatives which were implemented pursuant to that document have dramatically improved the technical interoperability of the network and its systems. Issues remain, however, regarding planning, funding and managing the assets so that they function effectively to support the department's needs efficiently.

The recently completed Review of Corporate Services Redesign, in the area of IM/TS, indicated that clients emphasized the need to consult with departmental managers. The analysis conducted in support of the Review of the Management of Information Technology suggests that there is also a strong need for program managers to consult with IM/TS staff in a wide range of areas. The most important of these areas is large scale computer based systems, and custom software applications.

It is also clear, however, that even day to day issues could be better coordinated and more effective if the management of information technology was based on integrated approaches. Large and complex initiatives, in order to be successful, should be developed and implemented with input from IM/TS, and in a way that is compatible with departmental approaches.

3.3.3 Large-Scale Systems

A study of existing large-scale systems in DFO was undertaken to measure implicit and explicit management structures in relation to large-scale systems that represent significant IT expenditures. This element of the review looked at large scale systems in the NCR and one Region (Maritimes). The purpose was to assess the management of these systems from conception to implementation or completion (where possible). Large-scale systems were defined as custom systems costing more than $500,000, delivered to more than 100 employees or implemented across multiple locations.

There is no single approach used within DFO for developing and implementing large-scale systems. In the public and private sectors, there are several planning and development models that have commonly proven to be effective in both controlling costs and bringing desired results. At least two of the DFO systems which this review looked at grew from an anticipated cost of less than $100,000 to an as-delivered cost of over $1 million (Departmental Violations Information System and the Habitat Referrals Tracking System). Overall, those that were developed through project-specific teams that included staff from IM/TS as well as program staff, end users of the system and consultants (where appropriate), tended to work the best. In other words, they were developed in harmony with the technical architecture and recognized and addressed the needs of the final user. Where detailed plans were absent, including specific milestones and clear descriptions of what a successful system would do, costs were high and in some cases deliverables did not appear in the year they were expected.

The infrastructure support of these large-scale systems as well as the evolution and maintenance of the systems themselves and user training must be addressed at the outset. In some cases, system support has been charged back to programs by IM/TS. When costs and levels of support were not explicitly agreed upon early in the process, discussions have been described as difficult.

When programs evolve very large systems, there is also a risk that they could implement networks which parallel the existing system. Certainly the existing Coast Guard inter-city digital circuits and the proposals associated with the INNAV project, from a hardware and architecture standpoint, are very similar to the WAN operated by IM/TS. GTIS is the supplier of inter-city links for the Coast Guard and IM/TS systems. In meetings with the review team, GTIS staff indicated that cost efficiencies could be achieved by consolidating the acquisition of these services. Clearly an assessment of potential savings from such consolidation is warranted. Indeed what travels through these systems and the fault tolerance of the activity are different and in while IM/TS buys services and Coast Guard leases digital circuits, however the hardware and inter-city links are in many cases similar, and the supplier is the same (GTIS).

In conclusion, a coordinated approach to the development and implementation of large-scale systems is a key improvement in governance which DFO should consider. These systems are not

only costly but, in some cases, systems to do the same thing are being developed independently in different sectors and regions (e.g. fisheries management information and licensing systems). The advantages of using an integrated, client-centered approach include cost savings as well as more robust solutions where experiences and approaches from one region or sector can be used to improve results in others.

3.3.4 Administration of the IM/TS WAN

This portion of the review looked at the management of the information "pipes" that carry information between buildings and cities. In computer parlance, the size of these pipes is called bandwidth and the usage is called load or bandwidth utilization. Like the pipe example, it is possible to "size" these links (the bigger, the more costly) and it is possible to fill them so full that the whole system slows and ultimately shuts down.

The links are made up of two general categories. The first of these is the WAN, which is managed and funded by NCR IM/TS. The LANs are the links managed by the regions from their regional headquarters. The complexity ranges from Central and Arctic, where all inter-city links are operated as WAN components, to the Pacific, Maritimes and Laurentian Regions where high capacity fibre optic and inter-city links are administered from the regional headquarters.

The IM/TS WAN, which links together 94 DFO computers (i.e., routers) across Canada, is the primary system for inter-city communication of departmental e-mail, desktop applications and data. The day-to-day administration of this network is contracted out to Public Works and Government Services Canada (PWGSC) Government Telecommunications and Informatics Services (GTIS) group. In 1998-1999, GTIS subcontracted management of the system to a local private firm called NUVO Networks.

Information surrounding the management process that resulted in GTIS' being awarded this contract suggests that customary procedures were not followed. Managers of regional LANs indicated that they were simply advised the service would be provided by GTIS, without input or consultations with the regional client organizations. The review team was advised that when the contract was awarded to GTIS, the DFO contract to manage 94 routers represented a doubling of GTIS' responsibility. The management of this award does not seem to reflect the type of consultation and coordination that is considered desirable. In addition, as noted below, there are several weaknesses in the current arrangements.

A review of the service level agreement for 1998-1999, as well as a series of interviews with DFO and GTIS staff, have demonstrated that there are weaknesses in the document. These include:

1. The services that GTIS must provide to DFO are not defined in detail, although there are direct references to network availability and action to solve specific problems.

2. GTIS measures its performance against the network availability criteria, but is under no obligation to report when the specified availability is not achieved. Furthermore, if the specified network availability is not met, there are no penalties or financial remedies for

DFO. The network availability would seem, therefore, to represent a "target" rather than a standard. A more binding service level would clarify what exactly DFO is purchasing and what consequences or actions flow from a failure to provide this service level.

These arrangements result in DFO receiving daily, weekly and monthly reports from GTIS/NUVO. These reports are so general, they have no meaning to either GTIS or DFO staff. While the total failure of any particular link in the network is reported to NCR IM/TS if it cannot be repaired within two hours in the business day, total failures are far more rare than overloaded conditions that slow down all communications including e-mail and Abacus sessions.

In addition, the reporting is not stratified so that the six links that are critical for inter-regional communication are shown separately. The Vancouver WAN link, for example, supports all network communication within the Region and with other Regions. Its failure therefore affects all 2,344 staff in the Pacific Region and the ability of the rest of DFO to reach them. This is an entirely different situation than would occur if the link to a small sub-area office failed and only the few staff in that office would be affected. The daily reporting system currently provided by NUVO treats these two links in an identical way.

A detailed analysis of the architecture of the network was conducted. The nature of the management of the LAN and WAN made it difficult to identify all of the equipment connected to the LAN/WAN. After a comprehensive "topology" was prepared, it was clear that the DFO network reflects its history of having been assembled by linking together a variety of sub-components, rather than having been designed as a whole.

GTIS, who is responsible for making architecture recommendations as a part of the current service level agreement, has not done so. The computer consultant who conducted this component of the review has indicated that DFO could achieve cost savings in network management costs and increases in security and performance if a consolidated department wide architecture were implemented. The failure by GTIS to provide architectural recommendations that would support increased performance and decrease costs, that are required by contract, is seen by the review team as a serious shortcoming. As the contract contains no penalty provisions, there would appear to be little that can be done to remedy this until this work is re-tendered in the subsequent fiscal years.

The effective management of "bandwidth" is one of the most apparent measures of service to clients. When network links become overloaded, the time taken for information to travel across the network increases. This is especially evident to users when mission critical applications like Abacus, Peoplesoft and, in some regions, Word and Excel, are delivered from a central location. If e-mail takes a few minutes or a few seconds, it is seldom apparent to users; however, if a user is entering data or preparing a report and it takes minutes to get a response from the application, users become frustrated and application-related problems can result. As a result, one network management function is to watch the level of "traffic" on network links and ensure that the level of service is good under "normal" circumstances.

The reports currently provided by GTIS to DFO report on only the ten busiest links. In several cases, these are situations for which no remedy exists that would overcome slow or overloaded

links, because the local telephone company has limited service to the area. In other cases where large inter-regional links become slow, there are no agreed-upon explicit steps to be followed. The current management of the WAN has three approaches that they use. An assessment of several examples has not demonstrated how one approach is chosen over another. The review team asked for written guidelines which would apply to these management decisions and was told that none existed.

When links become so busy that performance degrades, the options are to do nothing, to increase the capacity of the link, or to prohibit certain applications from being used. The first approach was apparent in discussions with IM/TS staff where they have indicated that for some small DFO offices, although increased capacity is required, there is simply not enough money to purchase the equipment and services to accomplish this. As an example of the second strategy, the capacity of six WAN links was improved in October 1998, demonstrating that in certain circumstances increased capacity is purchased. An example of the last strategy related to actions taken in regard to the WAN link connecting the Newfoundland Region to the rest of DFO. In that case, Abacus users in Newfoundland found performance across the WAN to be slow. Rather than doing nothing or purchasing greater capacity, a decision was made to shut down multimedia access to all users in Newfoundland, NCR and Central and Arctic. There was no consultation with or notification to network users of this change. Further, when adjustments are made to redirect Newfoundland Internet traffic through a regional firewall, it is not clear whether this multimedia access for NCR and Central and Arctic users will be restored.

GTIS is identified as responsible for identifying network links that are overloaded, identifying remedies to DFO and implementing remedies. Even though the SLA clearly identifies this type of analysis as GTIS' role, DFO staff routinely conduct this analysis and all of the recent link upgrades have been implemented as a result of the work of DFO staff, not staff from GTIS.

3.3.5 The Need for IT Support Outside Of Normal Working Hours

DFO's programs, especially those relating to emergency response, must operate effectively at all times. While many "mission critical" activities rely on the WAN/LAN, the historic approaches of fax and telephone serve to "back up" these WAN/LAN approaches. As technology moves more and more into an essential role, this ability to use "the old way" will diminish in effectiveness, thereby increasing the need to reduce single points of failure in the WAN/LAN. During this review, program managers often expressed concern that the increased reliance by programs on IT infrastructure requires that the WAN/LAN deliver completely reliable performance 24 hours a day, 7 days a week.

Currently only 6 of DFO's 94 routers are supported on a 24 hour basis. All other routers on the WAN/LAN are supported during the business day only. The Coast Guard inter-city links, where the program mission requires it, are supported 24 hours a day. In order to implement any consolidation of the IT functions currently found in Coast Guard and IM/TS groups, it must be assured that the off hour business needs of clients are fully met.

The threat and risk assessments recommended in the security section of this report can be used to identify if there are current WAN/LAN elements beyond those already supported that require 24 hour support. It would appear that the high reliance on e-mail, especially during emergency response to spills, marine accidents, and fisheries enforcement activities would make the e-mail system a candidate for 24-hour support. It must be noted here that, because of the costs of paying staff for standby and call-backs, implementation of 24 hour support in all regions could be costly.

3.4 NEED FOR POLICIES

3.4.1 General Areas Where Improvement is Required

A key general finding, which occurred across all lines of enquiry, was the need for the implementation of "who does what" and "how are things done" types of policy. In some cases, the limitation is the absence of applicable policy; in others, it is failure to implement an existing policy.

The general areas in need of relevant and meaningful policy guidance that is in line with program needs and user input are as follows:

1. LAN/WAN level of service commitments;
2. security of LAN/WAN equipment, desktop devices and data on servers and local machines;
3. fault tolerance in the LAN/WAN and e-mail, including tolerance of single points of failure and the requirement for 24 hour support;
4. LAN/WAN level of service to small offices, and very remote sites including ships;
5. criteria for evolution of the desktop office suite including the e-mail system;
6. acceptable use of Internet including any differentiation between use during and outside of normal working hours, and the degree to which DFO will serve as a general Internet Service provider for its staff;
7. the use of modems configured to auto answer on desktop computers connected to the WAN;
8. conditions under which a LAN may be set up to meet program needs;
9. departmental Internet firewall rules;
10. location of all network devices and the provision of uninterruptable power and backup;
11. extent and nature of support outside of normal working hours;
12. allocation rules for accessing bandwidth including a definition of when bandwidth use will be charged back to program areas;
13. consistent salary treatment of time spent working on DFO business on a DFO-owned computer linked to the DFO network outside of business hours;
14. identification of compatible hand-held computing devices, supported platforms and supported uses;
15. identification of what information types are to be placed on the Internet, and Intranet, and what types of information are not to be published in this way; and
16. a clear identification of the types of information that can be distributed by mass e-mail, and circumstances and mechanisms to direct widely distributed e-mail only to employees for whom it is relevant.

The absence of clear advice and direction extends to acquisition of "off the shelf" hardware and software, as well as to custom system development. In the user survey conducted for this review, a question related to "resources considered while making a purchasing decision" allowed the identification of multiple resources. Only 30% of those with purchasing authority consulted the DFO Informatics Architecture document, Help Desk or IM/TS staff before making a purchase, 38% consulted reviews in computer magazines while 72% consulted a knowledgeable colleague. In Maritimes and Laurentian Regions, there is strong pressure to use a robust planning process tailored to DFO's circumstances by DMR (a private computer consulting firm) before beginning a custom application development project. Even there, projects initiated in program areas often use only a portion of this DMR process.

The operation of the LAN/WAN system also exhibits wide variation in implementation and operation. As an example, in some regions, very tight control over Internet access can be contrasted with very few limitations in other regions. Similarly, there continue to be proposals to set up LANs and WANs entirely within program areas (e.g. INNAV, a recent Coast Guard initiative that is still under development). Should these proceed, the result would be that the same equipment running the same software, accomplishing the same "interlinking" objective would be done by two parallel organizations in the same department.

Even the serious training deficit identified by the user survey (40% of DFO staff want to have IT training, although the nature of the true need for training cannot be assessed by a survey) can be traced to the absence of a policy that calls for integrated implementation of new software and systems. This integration should include obligatory training as well as an assessment of network issues that may emerge. The recent partial roll-out of Office 97 has been associated with training issues (25% of DFO staff still want training on the desktop suite). It has also faced equipment compatibility issues. The Laurentian Region, presumably one of the main beneficiaries of the additional support for bilingual tools in Office 97, could offer Office 97 to only half of its users because of hardware limitations. Furthermore, the file incompatibility between Office 97 and its predecessor was identified by users as a major problem associated with this change in the desktop.

3.4.2 Want vs. Need

Microsoft's marketing department ensures that almost everyone in North America recognizes the phrase "where do you want to go today". In a business-computing context, however, a more relevant credo is where do you ***need*** to go today. DFO demonstrates the implementation of both models, the former being the more expensive, the latter being more appropriate in this time of temperate spending. The 1994 Price Waterhouse review of IM/TS clearly stated that "the solution [to too many half-done or unstarted projects] should be to do less, rather than continue to juggle conflicting resource demands".

DFO, through the Informatics Architecture process, undertook a comprehensive and necessary harmonization of hardware and software. If time had stood still, this would have been almost all that was needed. We began with a "work group" environment (where small groups of employees shared information among themselves and chose different word processors, operating systems and

e-mail systems). We have now moved to a "fully integrated" model (where communication across the department is facilitated through a desktop standard for file sharing, a single network operating system and a single e-mail system.)

The cost-effectiveness of PC computing over almost any other product group came about solely as a result of strong standards. When the public chose to see the IBM desktop system as a standard in a "Tower of Babel" environment, PC computing exploded. In less than twenty years, sales of desktop computers have gone from zero to 200 million units per year. As Bill Gates noted in his testimony in 1998 before the U.S. Senate in response to the Senate's assertion that Microsoft had operated in monopolistic ways, if aircraft costs and performance had followed the same price-performance curve as computing, "a 747 would cost as little as a pizza". Standards have been the key to efficiency and price competition, and offer DFO the opportunity to be efficient and cost effective in the area of IT.

The key question is how standards should be set for DFO that would be driven by clear program needs and the financial constraints that we face. It may be useful for us to consider what is necessary first and what may be desirable later. DFO could benefit significantly from a user-provider evolution of the Informatics Architecture standard. We are now in an environment that includes palm computers, worldwide digital satellite communication and sophisticated implementations of multimedia. None of these are considered in the architecture document but all now exist in various forms within DFO.

3.4.3 Evolution Of The Standard Office Suite

As a part of the Informatics Architecture process, a decision was taken to move to the Microsoft Office suite of products. This decision was made through a process that not only accounted for hardware compatibility but also included consultation with clients across all sectors. As noted elsewhere in this report this approach is considered to be a "best practice".

The next Canada-wide modification to the standard desktop was handled differently. In 1998, the desktop suite was upgraded from Office 4.3 to Office 97. This new version was purchased as DFO's national standard even though a business case had not been prepared showing the incremental benefits, and inventory information showed that a substantial number of users would be unable to move to the new standard because of limited PC memory and slow processors. In addition clients were not consulted on the need for any increased capability that Office 97 might bring. Only those users that had sufficiently fast computers were given Office 97, which left those operating Office 4.3 with file incompatibility problems with other DFO users. The current assessment that Office 97 does not run adequately on 486 machines, coupled with the cost associated with upgrading the hardware, suggests that this situation will remain until all of these machines are replaced. During interviews and discussions there were frequent reports of DFO staff receiving incompatible Word, Excel and PowerPoint files. An interim solution for management of this IT incompatibility problem exists and should be implemented.

A return to the business case model utilized in the development of the Informatics Architecture document is important, as Microsoft is continuing to evolve their desktop office suite and the

pre-release version of Office 2000 is now being sold to the public. DFO must ensure that future changes to the departmental desktop are done only after a full business case is developed. Office 2000 moves all key office functions into the Internet paradigm. Every computer in the network can "publish" documents, reports spreadsheets and presentations as Web pages. This is clearly a major change and should be subject to a full business case analysis including user needs, hardware and security implications.

There may be situations where the group of individuals working on documents together uses a different document standard than the standard for DFO. This is often the case in Science where collaborators are commonly from other scientific institutions. This is a likely explanation for the survey results which indicate that Lotus Word Pro and WordPerfect are found on some DFO machines. Clearly any departmental approach that is based on interoperability would recognize that within DFO the DFO standard would apply, and where other standards were appropriate, that DFO staff, in order to achieve a meaningful level of interoperability with collaborators, would have to have access to other desktop products, or other versions of the Microsoft products.

3.4.4 Internet – "Where Can I Go Today"

In this review, new IT-based approaches have been contrasted with the older "low tech" approaches to assess the management of the new against the management of the old. This is very difficult with respect to the Internet. Throughout this section, all references will be to Internet, not the internal government system called the Intranet. While the Intranet bears many similarities to its giant cousin the Internet, from a security standpoint they are worlds apart.

At the outset, it is important to note that we were unable to find an analysis or business case discussing the provision of full Internet access for all departmental employees. There are other federal institutions as large or larger than DFO (e.g. Revenue) where full Internet access is not provided to all staff. Certainly some DFO users, most often in Science, have been using the Internet since its inception.

In some ways, the "non IT" equivalent of the Internet is a library. The Internet has direct or indirect access to all kinds of information. It is instantaneous and anonymous and also is bi-directional. Furthermore, it is possible for individual Web sites to determine who has visited them and to find out technical information about visitors' computers. On the other hand, when employees visit a DFO library (the only generally available information source DFO provided for its staff prior to the existence of the Internet), they find that there is a carefully selected array of resources that relate to DFO's business as well as general sources of information including newspapers. In providing Internet access to all users in DFO, a far broader range of resources has been made available.

The Treasury Board Secretariat (TBS) is aware of this broad range of resources and has developed a high-level Acceptable Use Policy, which includes a recommendation that individual departments develop matching policies that relate more specifically to their situations. This policy calls for routine audits of departmental implementation. DFO has yet to conduct such an audit.

In the absence of an approved departmental policy, DFO has not monitored which Internet sites are being visited. Furthermore, while it is possible to "block" access to sites, at the moment only three of the firewalls have such blocking enabled. In all cases, the only use that is blocked is multimedia audio and video. This choice appears to be in conflict, however, with the transition of the departmental desktop standard to computers with sound cards and speakers, which provide the benefits of sound as an adjunct to the operation of the computers. In three regions and NCR, where this multimedia blocking has been implemented, users were not notified that the change was occurring (the fourth region with such blocking, Laurentian, advised all users of this change). The choice was made in the full knowledge that some remote DFO offices in the North would be blocked from their only access to CBC radio and that certain staff in the NCR were monitoring local radio in coastal communities. This blocking was done to reduce load on the network ("bandwidth") links between Newfoundland and NCR, while other network traffic to sites that are clearly unrelated to DFO's business remain open.

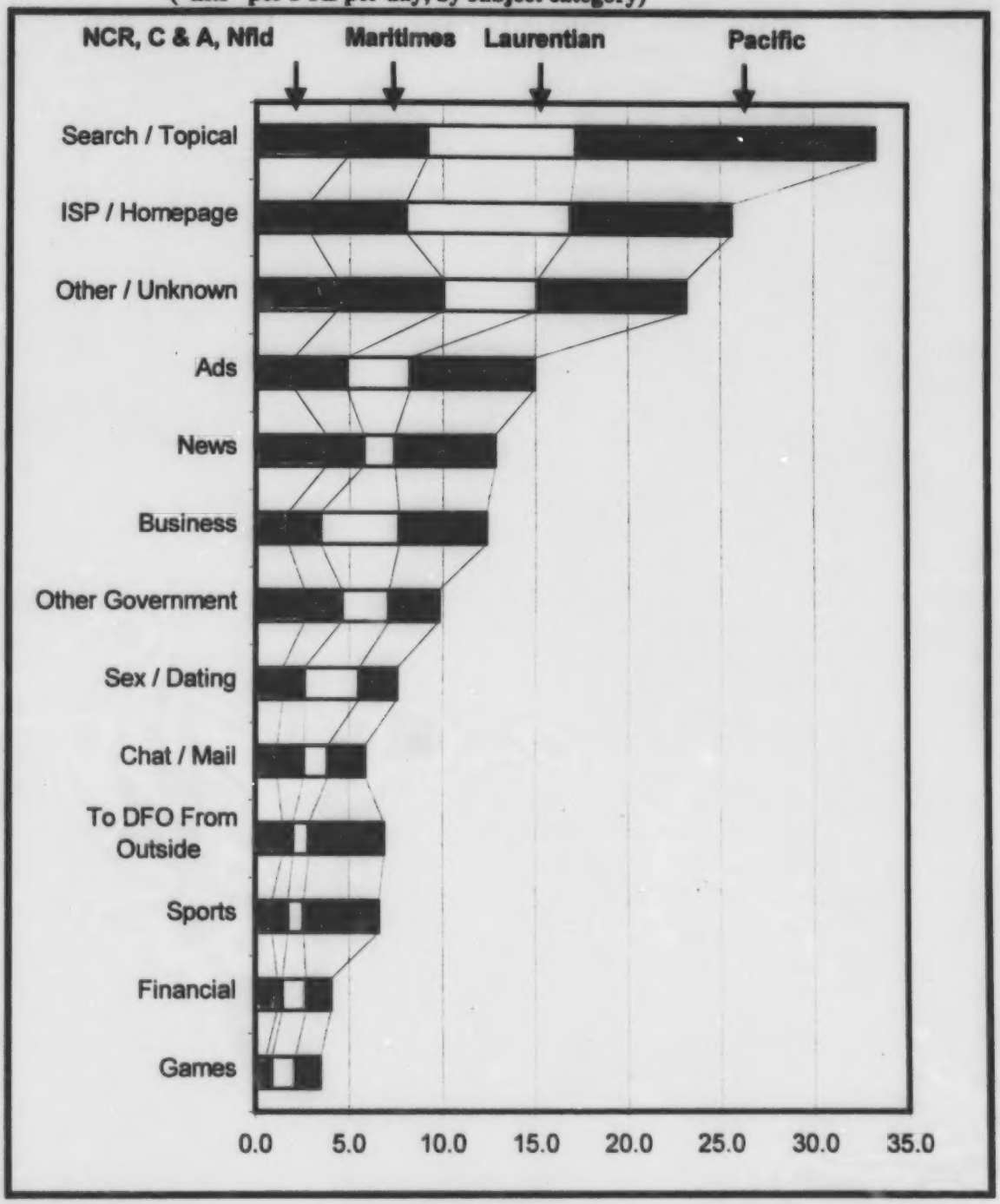
There is a further Internet inconsistency. While all DFO users have access to the Internet from their desktop, users in Maritimes who access the DFO computer from remote locations are given full access to all departmental resources, including the Intranet; however, Internet access is completely blocked (unless a specific use agreement is signed). Staff in NCR were subject to this limitation until the spring of 1999, when full Internet access was provided to remote users. No notice to users was made when this access was originally blocked and no notice to users was given when this full access to Internet was restored. DFO staff in Newfoundland, Central and Arctic and Pacific Regions who dial in to the DFO network have full Internet access. There is no policy basis for this difference. There is some concern that DFO staff dialing in from their homes would use DFO in the same way one would use a commercial Internet service provider. At the time of the review there was no DFO policy indicating that such use is unacceptable. An Acceptable Use Policy was issued on May 28, 1999 but is silent on remote access to Internet using DFO dial up lines.

A comprehensive analysis of Internet use by DFO staff in all regions shows that at least 10% of Internet traffic is to sites that are clearly not work-related. For each of the department's four firewalls that handle Internet access, the use was divided into 13 categories. The categories and their definitions are shown below.

To DFO From Outside	A DFO site: Coast Guard, Institute of Ocean Sciences etc. As this is firewall traffic, only incoming traffic from outside is shown here. Visits by DFO staff to the DFO Intranet can only be monitored on the 30 Web servers currently in use for this.
Other Government.	Other federal and provincial sites: National Research Council, HRDC
Search / Topical	Search and starting point sites: AltaVista, MSN
Business	Business related sites: Cambridge Scientific, ZiffNet
News	News sources: Canoe, newspaper sites
Financial	Financial sites: Banking sites, stock market sites
Chat/ Mail	Chat and Mail sites: Hotmail, Yahoo Chat
Ads	Ad sites: double click
Sports	Sports information sites: NHL sites, football and baseball sites
Sex / Dating	Sex and Dating sites: US Date, liveteen.com

Games	Game sites: Computer and other games; Sony Playstation site
ISP / Homepage	These represent user or other homepages such that the actual site visited can not be determined as many sites are hosted there. The ISP "Geocities" figures prominently, which is a site where music (MP3) files are found.
Other / Unknown	Sites where content could not be determined; no reverse lookup and / or the root page does not contain any site information or links. Eg: 209.143.228.181

Exhibit 3.4.4.1 One Week of Internet Traffic By Firewall
("hits" per FTE per day, by subject category)



This graph clearly shows that visits to government sites is low, when compared to generalized searches and "unknowns" (sites operated by the federal and provincial governments will, for technical reasons, not occur in this category). They also show that approximately 10% of the traffic is to sites with no apparent business purpose The actual average use of Internet was assessed as average number of Internet responses ("hits") per FTE per day. These are shown on the following table.

Region	Internet Hits per FTE per day
Maritimes	28.5
Newfoundland	28.9
NCR	
Central and Arctic	
Laurentian	42.2
Pacific	67.0

It should be noted that while users who dial-in from home in NCR and Maritimes have no Internet access, users that dial-in from their homes in Pacific, Laurentian and Newfoundland Regions have full access to the Internet. As the WAN/LAN and firewalls show low level of usage outside of normal business hours, and as Internet access is charged to DFO on a flat rate basis, it is not possible to identify costs associated with the use of Internet by users dialing in from their homes. One potential cost would be if additional dial-in "ports" were required to provide this Internet access from home. Pacific Region has half as many dial-in ports per FTE as the NCR, with twice the overall Internet use, so there is no evidence that additional dial-in ports have been installed to provide Internet access to DFO users from their home computers. The Acceptable Use of Policy issued on May 28, 1999, makes no differentiation between Internet use regardless of whether the connection is from the desktop or by dial-in.

The expenditures directly associated with the provision of Internet access are low when compared to departmental expenditures overall. It should be noted, however, that the "clogging up" of the WAN link between DFO and the rest of the department was, according the IM/TS staff, caused by extensive use of the Internet, and this use was characterized as related to the impeachment proceedings in the US. It is therefore important to note that Internet access across the DFO WAN/LAN can be a cost factor. The use of "non business related" sites either during or after hours was not a significant cost factor during the period which was monitored for this review. There would seem, however, to be management (salary/workload) issues which relate to overall productivity in the department. During the conduct of this assessment, no criminal use of the Internet was detected.

3.4.5 Access from Remote Locations

DFO requires remote connectivity for various purposes, including secure access from field offices, ships, teleworkers working from home, staff on travel status who need to access e-mail services and employees working from home outside working hours. As indicated in the user survey,

approximately 2,520 people access the DFO network from outside the office. Of this group, 650 people access the network from a DFO-owned home computer.

The user survey indicated that 65% of remote access users were satisfied with their remote access and 62% felt that such remote access was reliable. Overall, while the difference is small, respondents rated the ease of use of remote access slightly more favourably than the reliability of the connection/access software. The average rating for ease of use, using a 5-point scale, was 3.84, compared to an average rating of 3.71 for reliability. In general, these are positive ratings, indicating that remote access is generally working well. On average, Pacific Region respondents rated reliability the lowest. Fisheries Management and Science rated ease of use the lowest and Fisheries Management also rated reliability the lowest.

Remote access is delivered differently from region to region. Connectivity and speed of remote access varies tremendously nationally and within regions. There is no policy on who may or may not have (high capacity) Integrated Services Digital Network (ISDN) or digital lines; it is at the discretion of IM/TS, even if IM/TS does not fund these lines. A review of the management practices governing remote access found that record-keeping is unreliable. In some cases, staff were required to complete forms, while in other cases no paper or electronic authorization exists. Cross matching of actual records of remote access for one month against the approval forms confirmed that the management of this is uneven and controls are not visible. As was noted in the section on Internet access, there is inconsistent treatment of Internet access from remote locations. Policies, procedures, roles and responsibilities for remote access need to be clarified.

The management of IT as it relates to DFO-owned desktop computers in homes of the staff are also uneven. As noted above, the user survey indicated that approximately 650 people work after hours from home on DFO-owned computers. A review of the dial up user documentation could not identify that any of these individuals had entered into a telework agreement with DFO. A general management issue caused by IT is the differential treatment of overtime from these home computers. It is not clear if the provision of a DFO-owned (non-surplus) computer to a staff member constitutes implicit "authorization" of overtime or some form of employee benefit. It is not clear that DFO-owned home desktops are some form of (paid or unpaid) teleworking.

There is very little explicit implementation of "teleworking" where individual employees forego an office and conduct their work for the department during normal working hours from their homes. The few "teleworkers" now in place are generally utilizing this approach in response to health-related concerns, and for periods of less than one year. Given the funding pressures on the department as well as the flexibility which teleworking provides (where no formal office space exists for the teleworking staff member), a clearer management of this IT-created opportunity is desirable.

3.5 SECURITY

3.5.1 Threat and Risk Assessment

During the conduct of this study, the Coast Guard commissioned a study of secure network communications. While the scope of the study was restricted to the Coast Guard sector, and much of the analysis was inferential, this study and its threat and risk assessment provide a useful indication of the nature and impact of threats that exist for the DFO WAN/LAN system. The results of the Coast Guard's study was provided to the consultant conducting the analysis of the WAN/LAN for this review. Taken together several key areas for action have been identified. Specific areas of risk that require urgent attention are identified in the following subsections.

3.5.1.1 Architecture of Internet Links

An important priority has been assigned to Year 2000 compliance to ensure that critical DFO systems remain operational. However, it is equally important to ensure that our network is secure from other more current threats as well, especially from the Internet. Analysis suggests that some serious threats may exist from the manner in which access to and from the Internet is configured. While the Internet has provided quick access to a wide variety of information services, and enabled written communication (e-mail) to be as fast and as universal as the telephone, it is a very hazardous environment. Our interfaces with it (Internet firewalls) are managed unevenly and without the benefit of clear policies and rules. The net effect of this is that there are "more permissive" and "less permissive" sets of rules governing Internet traffic. The nature of a WAN/LAN is such that the least permissive firewall sets the level of risk for the entire system, even though there are six firewalls in DFO. Effective management of this aspect of IT again calls for a "business case" approach, as it does elsewhere. Certainly there are users that are accustomed to largely unfettered exchanges with outside users across the Internet. Such a business case analysis will assess how best to support real needs in a way that limits threats to the entire network.

The architecture of the electronic mail system was also identified as one with a high exposure to risk from Internet. The current system has some implementations where all mail, regardless of origin, is sent to mail servers that are inside the firewall system. On the Internet there are simple and readily accessible tools that can act as "mail bombs" and shut down entire-mail servers. If mail coming from the Internet was handled by a separate server (usually outside the protected area), then DFO internal mail could survive an Internet based attack. In some regions (e.g. Maritimes) the firewall is operated in such a way that problem mail (i.e. relaying of junk mail) is stopped at the firewall. This approach is not implemented on the NCR firewall, which passes all mail, including mail that calls for relaying.

In order for DFO to ensure its ability to conduct electronic business without interruption, the review recommends that a detailed threat and risk assessment be conducted specifically on Internet access and the configuration of the e-mail systems.

3.5.1.2 Protected and Sensitive Information

This review found no routine program that informed users of the security level of stored electronic information and electronic mail. The survey conducted as a part of this review indicated that of all shared services, the most valued is electronic mail. In many key areas, electronic mail has completely replaced the paper mail system for communications within DFO. While no study of the contents of electronic mail or electronic files was conducted, there is a risk that if not secret, certainly sensitive information (enforcement actions, personnel information etc.,) exists as electronic records in the DFO system. During the conduct of the review, the Coast Guard commissioned an extensive security study which found that the current mail system can be intercepted and modified.

The management of the use of electronic mail, now that it is the most common communication system in the department, requires that a full threat and risk assessment be conducted. While no evidence was found that Secret or Top Secret information was being sent in e-mail, certainly sensitive departmental information was being sent. The four categories for sensitivity of information are:

1) Very Low - That information, if compromised, could be expected to cause no injury outside the national interest (UNCLASSIFIED);

2) Low -That information, if compromised, could be expected to cause injury outside the national interest (PROTECTED A);

3) Medium - That information, if compromised, could be expected to cause serious injury outside the national interest (PROTECTED B); and

4) High - That Information, if compromised, could be expected to cause exceptionally grave injury outside the national interest (PROTECTED C) and information that, if compromised, could be expected to cause injury to the national interest (CLASSIFIED).

The consultant retained by the Review Directorate for this portion of the work assessed that our network was secure up to the Protected A level, as it was designed to be. While a further study could address this issue in more detail, during discussions with DFO staff it became apparent that there was no understanding of the "limit" to the sensitivity of information that could be sent electronically. There is reason to believe that information characterized as Protected B (which includes information that could be embarrassing to the department or sensitive information about DFO operations, staff or programs) is being transmitted over the current email system. While there are technical solutions (see 3.5.3 and 3.5.4 of this report) they are costly and would take time. A valuable first step would be to advise staff that electronic mail should not be used for the transmission of sensitive information. This would include, for example, e-mail which contained credit card numbers and the name of the authorized user of that card.

3.5.1.3 Access by Non-DFO Staff

The DFO WAN/LAN has three distinct groups of "non-DFO" users. The first are contractors and students and others who, during their tenure with DFO, are provided with user names and the types of access specified by the DFO supervisor or client. The primary risk here relates to closure of these accounts when this access is no longer appropriate.

The second group are federal employees of other departments who are located in DFO buildings. The department with the greatest presence is NRCan although Agriculture and Agri-Food staff also have access. The Natural Resources Canada (NRCan) staff are, for the most part, located in the Bedford Institute of Oceanography and the Institute of Ocean Sciences. At the Bedford Institute, their desire for a more open exchange with the Internet than the Maritimes IM/TS permits has been resolved with the NRCan staff having their own Internet access and no access to the DFO WAN/LAN. At the Institute of Ocean Sciences , however, permissive firewall rule changes have been made which bring some risk to the WAN/LAN. If staff from other federal departments find that they need a level of access broader than DFO permits for its own staff, then clearly a business case should be made, and the risks and benefits need to be explicitly assessed. The review found no such business cases during this review.

The third group of non DFO users can be found at the Canadian Coast Guard College. The College is now training staff from countries around the world. In the course of their work they utilize the department's IT infrastructure both in supervised classrooms and in unsupervised situations in common areas and their residences. While there is a firewall between the Coast Guard College and the DFO WAN/LAN, it is currently used to limit traffic from the DFO WAN going into the College, rather than being used to limit access from within the College. The Coast Guard College also operates an Internet firewall and has implemented rules that allow unlimited access out but severely restricts incoming traffic. In addition, the architecture of the Coast Guard College e-mail implementation is conservative and resistant to some of the risks that are evident in other parts of the WAN/LAN. The rationale given for implementing a firewall between the Coast Guard College and the rest of DFO was that the current DFO WAN/LAN did not provide adequate security from tampering.

3.5.1.4 Auto Answer Modems

DFO staff have used computers in their homes to conduct the work of the department for some time. Prior to well established networks and the type of high speed telephone access now available, DFO staff who wished to work from their homes could telephone to their office computer from a computer in their home (or other remote location like a field station or a hotel) and connect the two computers directly. This was done through a device called a modem (modulator/demodulator) which allowed the DFO desktop machine to "answer" the incoming call and give the remote user access to their own machine as well as the DFO Network. In the current environment with reliable high speed dial-up access and Internet electronic mail, the requirement for these modems is reduced. Nonetheless, where these modems are left on after work hours, and have inadequate security systems in place, they can represent a way for unauthorized users to gain access to the entire DFO WAN/LAN. While configurations do exist (e.g., dial back, where the modem calls out

to a single phone number known to be the users authorized location), there is no policy to require this type of configuration.

In order to manage this IT based risk a simple test can be conducted. A first step to identifying the degree to which such "auto answer" modems exist on DFO phone lines would be to "sweep" all DFO lines during the silent hours and identify which lines respond with an electronic handshake. When this list of "answering" phone lines has been created, and fax machines have been removed, the users of this type of "dial-in access" can be identified, and steps can be taken to ensure that adequate security is in place. At a recent meeting of the Institute of Internal Auditors, these auto answer modems were identified as the most serious security risk to the banking system worldwide.

3.5.2 Physical Security of Assets and Information

Securing IT assets physically is identical to the process used for other valuable assets in the department. One peculiarity is that computers (including servers and workstations) can almost immediately be broken up into components that are indistinguishable from newly made components. Another more important aspect is that the information that resides on the computer may be lost forever if it is not "backed up" to tape or the network. There is a further risk for those computers which play a significant networking role (servers, routers, name servers etc.) that contain information that would be useful to those trying to "break in" to the DFO WAN/LAN.

DFO has lost information and computers due to conventional theft. In one case, a departmental employee, upon leaving DFO, took a computer tape of catch data, which he used as the basis for opening a consulting business. Based on prevailing copyright law at the time, the only crime, as it turned out, was the theft of the tape itself, which was valued at less than $50. In other cases, desktop computers and memory inside the computers have been stolen. Security staff have noted that, while the theft of computer memory chips was a serious problem three years ago, it no longer is. This is attributed to decreases in computer memory costs rather than any change to physical security. When DFO offices have been occupied by protesters, there also have been cases where computers were damaged or destroyed.

Most LAN and WAN equipment is secured in computer rooms with combination locks. While this seems secure, often the walls of the room are drywall and can be easily removed. Most major DFO offices have video monitoring of entrances and exits. While this does not prevent theft, it may deter some thieves. In 1996, the server room at another Government department (the Journal Towers situated across from DFO headquarters at 200 Kent Street) was completely emptied of equipment in less than two minutes with full video coverage; however, no one was ever caught.

There is merit in concentrating network machines in areas with not only good physical security but also appropriate back-up power, cooling systems, and fire suppression. Given the nature of network computing and the general reliability of the telephone system (over which even "internal" network traffic travels), it would be possible to locate all "mission critical" LAN/WAN equipment in fewer physical locations than is now the case. In several cases, program areas (e.g., Coast Guard, Science) have their own computer rooms as well. There is merit in assessing where cost savings or improved reliability could flow from a reduction in the number of locations.

Currently, strong physical security of desktop machines (e.g., cabling them to desks; using more expensive case locks) does not seem warranted. Laptops represent a potential for loss of equipment or data for those who travel, but the review did not uncover any evidence that this currently is a serious problem in DFO.

3.5.3 Secure Authentication, Encryption and Public Key Infrastructure (PKI)

Currently DFO is assessing the need for IT solutions that would ensure that e-mail can be proven to have come from the apparent sender, and ways to prevent knowing the contents of or tampering with electronic information on the WAN/LAN.

As a business case for this has not yet been developed, it is sufficient to note that the only concerns expressed by Treasury Board Secretariat relate to securing transactions conducted pursuant to the *Financial Administration Act*.

The paper system that we now have has the capacity to meet TB's requirements as long as the transactions remain on paper. Furthermore, as long as remote access is by dial-up into DFO devices, the security risks of the Internet are avoided. While the implementation of secure authentication and encryption tools is an inevitable step, it can be entered into slowly enough to allow for a full analysis. A Revenue Canada analysis of options shows choices ranging in price for the first five years (based on 30,000 users) from
$3.2 million to $10.1 million.

Corporate Services IM/TS staff in Laurentian Region have looked into this in the DFO context and may have helpful experience from which the entire department can benefit.

3.5.6 Security and Internet - Firewalls

The Internet is bi-directional (i.e., we can get information from the outside and, under certain conditions, others can get inside if not prevented). As a result, we need a "gatekeeper". We use a "firewall" which is a mechanism used to protect the DFO network from unwelcome visitors, as well as to keep records on the information passing in each direction. The firewall basically is a sophisticated computer that uses specific software to conduct these gatekeeping functions.

Firewalls govern what activities can pass through with the ability to allow certain things "out but not in" and the reverse. In a system where several firewalls play a gatekeeping role to the same system, it would seem to be important that they are managed according to a standard approach. The department has six firewalls (Maritimes, Laurentian, Newfoundland, NCR[11] and Pacific Regions and the Coast Guard College). Three of these (Newfoundland, NCR and Pacific) are managed from Ottawa through a contract with GTIS and the other two are managed regionally.

[11] Internet traffic from Central and Arctic, as well as for Newfoundland non-Science users, travels through the NCR firewall.

The Coast Guard college manages their own. None of the firewalls has the same rules and there is no handbook or policy to govern what should be done.

How these rules are managed coupled with how "servers" are managed within the department is important. Twice in 1998, Science servers have been "taken over" by an individual from outside of government who used them to send up to 33,000 pieces of Internet junk mail per day (colourfully referred to as "Spam", after the luncheon meat of the same name). On the days that this occurred, it represented over 50% of the traffic on the firewall. Furthermore, in November 1998, an individual obtained broader unauthorized access to DFO systems and unsuccessfully issued instructions to DFO devices 300 times in one day. Firewall records indicate that attempts to enter our system without authorization are continuing. A management issue exists here as GTIS agrees that it is their responsibility to look for indications of Internet based attacks (called "probes") and to take action: however, they indicated that this is not being done. Pacific Region IM/TS staff discovered probing in the fall of 1998 and identified and took the necessary steps to ensure that these particular probes would be unsuccessful.

The implications are clear. In the spamming incidents, an unauthorized user gained access and issued instructions to a DFO device to send junk mail. Once inside the firewall, other more harmful results could have happened (e.g., changing or erasing data, access to other open servers in any region, installing a program that could look into e-mail messages, etc.). These harmful results are inevitable unless some important steps are taken. These steps include a threat and risk assessment, a clear statement regarding the level of risk to the system that can be tolerated and a suitable approach to limit risk where stringent access cannot be implemented for program reasons. The costs to the department will vary based on the level of risk and the acceptable amount of time certain functions like e-mail or an inter-city link can be out of service.

The department clearly needs general agreement as to how these firewalls are configured. A review of the change requests to firewall rules also points out that the system for rule changes is uneven. For two of the firewalls (Newfoundland and NCR), there is no audit trail within DFO to verify that the contractor (GTIS in these cases) has complied with requests. There are also three different firewall systems in place and even the three firewalls using the same software are each using different versions. This makes the day-to-day management as well as coordination among the firewalls very complex. There is a plan to move all firewalls to the same system, but this has not yet been done. There is also a move to have all six firewalls managed centrally; however, if there are standard policies and approaches, there is no technical need to eliminate the regional management of regional firewalls. It should be noted that when information on firewall rules was requested, the regional firewall managers in Laurentian and Maritimes were able to respond in one day while GTIS took over four weeks to respond to the identical request. This is another example of poor performance for which the 1998-99 contract provided no remedy.

While there are some needs (e.g., in Science) to collaborate openly with specific colleagues outside DFO, where such collaboration brings risks to the LAN/WAN, it must be assessed more broadly. The option exists for such machines to operate separately from the LAN/WAN or to implement an approach such as PKI. In some cases, it may be that this collaboration can be accomplished in a way that eliminates risk to the network as a whole.

3.6.7 Elimination of Single Points of Failure for Critical Systems

The heavy reliance by programs on IT for support is moving DFO to a position where the failure, for even a few hours, of inter-office or inter-city communications or access to core applications (e.g., e-mail) can cause serious disruption. A concerted effort to ensure that core functions are identified and that single points of failure in these systems are eliminated is critical in ensuring that key departmental roles (e.g., search and rescue, oil spill trajectory monitoring, etc.) are available at all times. Where merged administration of Coast Guard systems is considered, it is critical to note that many of their navigation and search and rescue functions cannot tolerate failure. This is very different than general e-mail, word processing and financial functions where a 24-hour delay can often be tolerated.

Recently regional IM/TS staff at the technical level have struck a working group to help find solutions in many of the foregoing technical areas. This is a valuable step and with the inclusion of IM/TS NCR staff and representatives of clients, simple workable solutions may be found in these and other important areas.

3.6 COMMUNICATIONS

3.6.1 Communication Channels

The management of IT based communication is in line with the patterns for other areas. There are few, if any, national standards and where these exist, they are not visible to users. As well, with few exceptions they been developed without input from users/clients. DFO uses all electronic communications channels, from mass e-mail through to Intranet, Internet and public folders. There is, however, little evidence of a clear fabric of policy indicating which system will be used for what and which communications are not appropriate for electronic distribution. The net effect of this is that every channel is used. While the management of the elements of IT that link to communication (mass e-mail, Internet, Intranet, and public folders) are all delivered with IT, they represent approaches that, if conducted on paper (letters to all staff, departmental and regional newspapers, etc.), would be managed completely within the domain of the Communications Directorate.

There is some evidence that staff are experiencing information overload. A survey conducted in 1997, during the development of the departmental Operational Greening Plan, showed that staff did not find mass e-mails, even those signed by senior staff, a valued way to obtain information. In the NCR, there were over 450 mass e-mails in 1998, ranging from job offers to a specific group and level to warnings of fire alarms on week-ends when few staff are present. An informal study conducted in Pacific Region indicated that there had been an average of 5 per day in 1998.

There is a need for compatibility, consistency and quality of information both within and among the regions and branches. The many options (Intranet, mass e-mail or public folders) make it very difficult to choose the right medium for delivery of information. Programs are at a loss to know which medium they should use to communicate. There is neither policy nor any evident source of advice that one can turn to. Public folders, what they are and how to use them, are a mystery to

most departmental staff. The content of mass e-mails needs to be examined as to whether it is information that could be transmitted using another medium (such as e-mails about parking to only those who use it).

3.6.2 Web Publishing

The management of publishing information on the Intranet and Internet can be found not only in the Communications Directorate but also in program areas across the department. Web publishing has become a widespread activity since the emergence of the "hypertext" language, which permitted linking text in one document to other information resources like maps, tables, and other reports. This has been further enhanced by the development of fast "global" searching engines capable of examining millions of records for one specific piece of information. It is in fact another channel of communications, but one which is sufficiently large that it warrants special attention. This is especially true since the Internet has the potential to become an even larger expenditure. Industry Canada has implemented a small business outreach Internet activity, called "Strategis", which has cost over $20 million to implement with annual operating costs of several million dollars per year. PriceWaterhouseCoopers, in its publication *"Technology Forecast: 1998"*, indicated that large Internet presences routinely cost over $10 million, with electronic commerce sites (like Amazon.com, the world's largest bookstore) costing over $30 million to develop and $5 million per year to maintain because of the high costs of providing constantly changing information. While some may argue that DFO could benefit from expenditures as high as $15 million in Web publishing, no business cases were found for any of the current Web publishing activities.

This review identified that DFO spends approximately $2 million a year on Web publishing costs, including hardware, software and salary expenditures. In the survey of DFO staff, 72% of respondents indicated that they had used the internal Intranet in the previous month. The usefulness of information obtained was rated at about 4 on a scale of 5. Furthermore, 82% reported that they used the Internet at work. Some key DFO information that is for clients (such as statistical reports and fisheries regulations) is now available solely on departmental Web servers.

A very real potential exists that non-scrutinized material has been and will be mounted on Web sites, both for public consumption via the Internet and internal viewing via the Intranet. No wide-ranging controls exist to verify that the material is accurate and in stride with DFO policies and mandates. While the Communications Directorate has the responsibility for enforcing Departmental and Treasury Board standards, they indicated that they had not done any monitoring. Indeed the Pacific Region Web pages coraply with neither the Departmental nor the Treasury Board "look and feel" standards.

From an efficiency point of view, no mechanism exists to ensure that Web-published material is valuable. This is a highly voluntary activity at DFO, relating more to want than need. Many groups admit to publishing on the Web "because it is fun." The majority of Web publishers do not have a clear idea who their audience is and this makes it difficult to decide what to include and what to exclude. Even when a study was done with contact groups, over 80% of the clients in the contact

group had had no experience with the Internet at all. As Web publishing tools become cheaper and easier to use, it is probable that more and more material will be mounted for public viewing.

There are a couple of notable exceptions to this: a lot of Web page development in the Maritimes and Laurentian Regions has been adequately planned. Region-wide committees were struck in these Regions with an eye to defining the client and presenting more narrow, pertinent groupings of information. Such approaches represent a "best practice" and a management approach that should be more widely implemented.

3.7 TRAINING

3.7.1 Training Deficit

The management of change in the area of IT appears, from survey results, to have inadequately managed the training component. The user survey undertaken as a part of this review found that 40% of DFO employees would like training for software currently installed on their computer. The same survey indicated that approximately 2,970 people at DFO have not received training when new software is installed and half of DFO employees (approximately 4,500 people) have not been advised of the uses or benefits of new software that has been installed. If this is addressed, a number of issues related to ease of use, reliability and reliance on the Help Desk would also be mitigated. While IM/TS staff point to the numerous courses that are offered and Intranet pages describing what courses are available, the survey results indicate that these approaches have not been effective in reaching the 50% of staff who appear to still want training.

Computer users want more training than they have received. This presumably is partially a program decision, somewhat independent of IM/TS. Training on the office suite was identified in the survey of departmental users as a need by 25% of departmental staff; however, IM/TS is offering training and commercial training is also available in every major city. The fact that program staff feel the need and have not received training on the office suite suggests that staff have not asked for training or that managers have not allocated funds to address this.

One effect of the absence of training on applications as widely implemented as the office suite is that the Help Desk function becomes burdened with simple and unnecessary requests. The Pacific Region, in moving to a Help Desk offered by internal staff rather than contractors, indicated that it was not prepared to pay a contractor $37 an hour to provide basic problem-solving in the use of Word. There are a number of other ways that this problem could be addressed. A number of management approaches are available. One approach would be to direct software-related calls to a service organization that solely does software support and may charge less than our internal costs. A second way would be to limit the number of "software operational" calls for individual users (e.g., four "office suite calls per person per year"). A third approach would be to monitor the exact nature of Help Desk calls and report this to one of the IT user/client committees for action. In some organizations there is an internal charge back system on a per call basis. This approach brings the training/help desk cost directly to individual program managers.

Clearly, the evolution of the desktop triggers a need for training. Whenever core software is changed to add new features that affect the users and require new skills or training to utilize, the costs of and arrangements for training should be established before any new versions are purchased. Given that Office 97 is still not fully implemented, consideration of the new operational demands associated with evolving the national desktop standard to Microsoft Office 2000 (currently being sold as a pre-release version to the public) should be detailed and comprehensive. This is especially true as a number of large corporations have made a needs-based decision to continue to use Office 95 (essentially the version that DFO is still using on the 486-based computers) and avoid the training, hardware and technical incompatibility issues associated with Office 97. As there was no business case analysis showing that Office 97 was required in order for DFO users to deliver their program responsibilities, the many hardware and software difficulties which accompanied this change could have been avoided.

Where specialized software (such as the Departmental Violations System, Habitat Referrals Tracking System, Abacus and others) have been rolled out, the record of staff taking training is better. It may be that managers consider office functions routine and recognize that custom applications require specialized training. Alternatively, managers of program-based systems may feel a clearer ownership of all aspects of the implementation, including training.

In the Pacific Region, there was an innovative implementation of the Office 97 desktop. A "per user" package was created and "sold" to managers for $125 per user ($100 was the cost of one half-day of training and $25 was a contribution to the cost of the software license and the accompanying CD-ROM). The full cost of the Office 97 software license was $78 per user, three times the recovered cost. Although Pacific IM/TS originally intended to offer only "complete" packages which included the training, it eventually bowed to program pressure and "sold" licenses without training to program areas at $25 per desktop. This resulted in the new software appearing on the desktops of program staff without staff having been trained in its use. The user survey results for this review confirm that program staff still wish to have this training. A business case approach, even in this case, would have allowed for better management of this IT transition.

New versions of office "desktop" software are often acquired to gain access to new features not found on older versions. It is important to assess through client-provider committees what program needs exist for these new features. Furthermore, the training necessary to use these features must be included in the consideration of costs and benefits. In the example outlined above, taking the $100 per user used by Pacific Region as a reasonable cost to the department for Office 97 training, the Office 97 license itself cost $700,000. However, it created a program need for training of $900,000 (9,000 employees at $100 each), making the actual (non hardware-related) cost $1.6 million. In all future system-wide upgrades, the costs of training must be included in the business case that supports the change. Training needs to be made a part of every change to the system and training for existing and new versions of e-mail and the desktop suite should be considered as a part of network costs.

The case has been made that often new and expensive changes, while not required by users, make the IM/TS functions easier to conduct. This does not diminish the need for a full analysis of the benefits and costs (including disruption, training and new hardware) that would accompany such a

change. Certainly Microsoft is holding free seminars on Office 2000 for IT managers saying it is easier and cheaper to manage than the current Office 97, while at the same time remaining silent on the new hardware requirements and interoperability issues. As noted elsewhere in this report, a business case analysis considering products from a variety of manufacturers should precede investments of this type.

Finally, the user survey identified that between 12% and 28% of departmental staff have "given up" trying to solve a computer problem which they feel impairs their ability to perform their responsibilities. It is likely that this would be reduced if the requested training (40% of staff) were provided.

4.0 Recommendations

It is recommended that

4.1 The department move quickly to implement a decision making process that will ensure that investments in IT are fully assessed, both for their support of the program needs of the department and for their compliance with departmental standards and architecture. Such a system should clarify accountabilities for the management of all IT assets, services, standards and architecture. This process must include IM/TS staff and clients, from all regions and the NCR. The process used to develop the Informatics Architecture document is a good model.

4.2 The department ensure that large scale IT systems are assessed using a comprehensive project assessment and planning tool. Maritimes and Laurentian Regions use a system that was developed for use in DFO and has proven helpful in ensuring the smooth implementation of large scale systems.

4.3 The department establish reliable long term funding for the IT components which are fundamental to communications and interoperability. This includes the telecommunications, hardware and software that support the WAN/LAN, as well as the standard "desktop office suite" and e-mail system. Funding for staff who operate and maintain this system (either directly or under contract) as well as the "Help Desk" and "portfolio management" staff should be included. The level of ongoing funding should recognize the rapid rate of change that is characteristic of IT, while at the same time focus on what is required for DFO to deliver its program responsibilities.

4.4 Corporate Services IM/TS conduct a Threat and Risk assessment of the network with a high priority on assessing threats from the current architecture of Internet access to DFO to determine if they represent an acceptable level of risk.

4.5 Corporate Services IM/TS in the Regions and the NCR work together to identify the products and services, including reports, acceptable response times, and levels of service that are required for the operation of the WAN. This should be used to obtain, by tender, telecommunications and network assessment and reporting services for subsequent fiscal

years. Further, a complete assessment should be carried out of the products, services and levels of service that should have been provided by GTIS under the current arrangements, but were not. Should the service deficit that this analysis identifies be substantial, remedial action should be taken.

4.6 Corporate Services IM/TS take steps to notify users of the security of DFO's current electronic systems, and the degree to which they should be used for sensitive information. An assessment should be conducted to determine the extent to which DFO needs secure encryption and authentication for e-mail and financial transactions.

4.7 Corporate Services IM/TS develop, in cooperation with programs and departmental human resources staff, a mechanism to address the "training deficit" identified in this review. Over half of this "training deficit" is related to the operation of the current "desktop suite".

4.8 Corporate Services IM/TS in Regions and the NCR work with clients to establish reasonable and effective means for standardizing:

4.8.1 Acceptable levels of network performance
4.8.2 Firewall Rules
4.8.3 Levels of service to small offices, remote locations and ships
4.8.4 A mechanism for assessing the evolution of the desktop standard and e-mail
4.8.5 A suite of policy statements in the areas identified in section 3.4.1 of this report
4.8.6 What services and areas qualify for 24 hour support
4.8.7 What services and areas must have no single points of failure
4.8.8 Chargeback and support arrangements for program based large scale multi-region IT initiatives
4.8.9 IT and WAN/LAN services provided to tenant departments (e.g. NRCan)

4.9 Corporate Services IM/TS develop an effective and comprehensive needs statement for the WAN, which would include clearly stated performance criteria, reporting requirements based on the needs of IM/TS staff in NCR and the Regions, and penalties for failure to perform according to specified standards and use this as the basis for contracting for the WAN services so as to avoid the many weaknesses identified in the current arrangements.

4.10 Steps taken by regional Corporate Services IM/TS staff to work towards addressing architecture and firewall inconsistencies be expanded to include NCR staff and clients so that a comprehensive solution that recognizes client needs can be implemented.

4.11 Corporate Services IM/TS and the Communications Directorate work together to identify an orderly and reasonable approach to the use of electronic communications and information sharing. Consultations should include program areas that currently sponsor Web publishing both internally and on the open Internet.

4.12 The Coast Guard, in cooperation with GTIS and Corporate Services IM/TS, assess the degree to which program needs can be met and savings can be achieved through

harmonized acquisition of telecommunications services. Such an assessment is especially desirable given the technical similarities of the soon to be implemented INNAV system to the equipment and links currently operated by Corporate Services IM/TS.

4.13 Corporate Services IM/TS advance the Acceptable Use Policy for IT resources so as to provide clarity on what is, and what is not acceptable for DFO employees. (Policy was issued May 28, 1999).

ACKNOWLEDGEMENTS AND THANKS

Special thanks are due to the staff of Corporate Services IM/TS in the NCR and in all regions. A special vote of thanks is due to the Director General, IM/TS, who throughout the exercise worked hard to ensure that the review team had the information that it required. In addition, several IM/TS Directors and many staff from the technical and support side of the informatics function have taken time to make helpful observations, review draft findings and explain the intricacies of a complex system.

5.0. MANAGEMENT ACTION PLAN

The Context of The Review

Fisheries and Oceans has a complex array of missions reliant on information technology for a number of key aspects. This reliance, coupled with the geographic scope of the department, has resulted in early and continuing investment in information technology.

Science, as an activity, has used computers since they first became available. Certainly some of the pivotal and ground breaking uses of computers to compile and analyze large volumes of information were done by DFO Science staff. Further the scientific community was the foundation on which the Internet was based. DFO Science staff use the Internet for communication and collaboration with scientists around the world and have done so since this first became possible. Similarly the distribution of information to clients and to the academic community is heavily reliant on information technology.

The Coast Guard, because of their responsibilities for navigation and search and rescue has also been on the forefront information technology. Information flows related to navigation and safety come from all parts of Canada, from remote light stations to busy harbours.

DFO as a department has also been an early adopter of communications, analysis and delivery mechanisms that are based on information technology. The implementation of a national electronic systems for mail, financial and human resource systems is evidence of this. The survey conducted as a part of this review found that virtually all respondents (97.4%) reported that they had access to or used a computer in their regular work activities. Department-wide access to computers appears to be consistent, as at least 90% of respondents in all regions and sectors indicated that they use a computer in their regular work activities.

DFO has made, and continues to make major investments in information technology. During the period of the review DFO was spending $6,650 per employee per year on information technology. This review has identified and made recommendations on important areas for action. When the recommendations found in this report have been implemented, a better and more cost effective use of information technology will result.

5.0. MANAGEMENT ACTION PLAN

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
1. The department move quickly to implement a decision making process that will ensure that investments in IT are fully assessed, both for their support of the program needs of the department and for their compliance with departmental standards and architecture. Such a system should clarify accountabilities for the management of all IT assets, services, standards and architecture. This process must include IM/TS staff and clients, from all regions and the NCR. The process used to develop the Informatics Architecture document is a good model.	The ISC has now been established and has recommended a departmental informatics project proposal review process. This will provide for a corporate review of project proposals with a view to reducing risks, assessing conditions for success, reducing duplication, and leveraging the results in support of the strategic directions and business priorities of the DFO. Our strategy is to implement the approval process for larger scale system initiatives, to prove it right and valuable, and then to implement similar processes (at other levels and perhaps on a smaller scale) for smaller initiatives. In the meantime, the model is being assessed for use within several regions and sectors.	Director, Planning and Information Management Services Branch	September 1, 2000
2. The department ensure that large scale IT systems are assessed using a comprehensive project assessment and planning tool. Maritimes and Laurentian Regions use a system that was developed for use in DFO and has proven helpful in ensuring the smooth implementation of large	For large scale IT projects, Application Services Branch (ASB) will promote the use of two key Project Management skillsets *Software Project Planning* and *Software Project Tracking and Oversight*. These Project Management processes are an integral part of the Treasury Board Enhanced Management Framework (EMF). They will be promoted by ASB through seminars in NCR and in the regions using the EMF as the framework. ASB	Director, Application Services Branch	ASB training & seminars have started. June 2000 at the latest for tool kit recommendation.

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
scale systems.	staff members are currently being trained on both and are being encouraged to pursue Project Management Certification. Project Management tools are also being evaluated. We will propose a standard tool kit for project management to DMC/DEC.		
3. The department establish reliable long term funding for the IT components which are fundamental to communications and interoperability. This includes the telecommunications, hardware and software that support the WAN/LAN, as well as the standard "desktop office suite" and e-mail system. Funding for staff who operate and maintain this system (either directly or under contract) as well as the "Help Desk" and "portfolio management" staff should be included. The level of ongoing funding should recognize the rapid rate of change that is characteristic of IT, while at the same time focus on what is required for DFO to deliver its program responsibilities.	➢ Submit option analysis and recommendation to ISC/DMC for decision regarding the on-going A-Base funding requirements for the DFO Shared Informatics Infrastructure addressing consistent and reasonable service levels throughout the Department.	DG, IM&TS	January 2000 -- A-Base has been revised, and we are developing a DFO-wide cost-recovery strategy for informatics. Target: June 2000
	➢ Submit the Shared Informatics Infrastructure capital refreshment requirements included in the LTCP to DMC for funding approval.	Director, Planning and Information Management Services	Fall 99 -- requirements have been submitted. LTCP not yet finalized & approved.
	➢ Ensure that national and regional IM&TS organizations participate fully in the DFO Business Planning process, and LTCP asset	Director, Planning and Information Management Services	Fall 99 -- all have participated

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
	identification, refreshment, investment and planning process.		
4. Corporate Services IM/TS conduct a Threat and Risk assessment of the network with a high priority on assessing threats from the current architecture of Internet access to DFO to determine if they represent an acceptable level of risk.	Corporate Services IM/TS will conduct a full threat and risk assessment of the national infrastructure including the location and policy structure on all firewalls and the architecture of the electronic mail system by September 1, 2000	Director, Technology Services	September 1, 2000
5. Corporate Services IM/TS in the Regions and the NCR work together to identify the products and services, including reports, acceptable response times, and levels of service that are required for the operation of the WAN. This should be used to obtain, by tender, telecommunications and network assessment and reporting services for subsequent fiscal years. Further, a complete assessment should be carried out of the products, services and levels of service that should have been provided by GTIS under the current arrangements, but were	Corporate Services IM/TS in the Regional and NCR will work to identify the products and services including reports, acceptable response times and levels of service that are required for the operation of the WAN.	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
not. Should the service deficit that this analysis identifies be substantial, remedial action should be taken.			
6. Corporate Services IM/TS take steps to notify users of the security of DFO's current electronic systems, and the degree to which they should be used for sensitive information. An assessment should be conducted to determine the extent to which DFO needs secure encryption and authentication for e-mail and financial transactions.	Corporate Services IM/TS will send a reminder to all users of the email system every quarter reminding them that this system should not be used for secure or sensitive transmissions.	Director, Technology Services	September 1, 2000 and ongoing
7. Corporate Services IM/TS develop, in cooperation with programs and departmental human resources staff, a mechanism to address the "training deficit" identified in this review. Over half of this "training deficit" is related to the operation of the current "desktop suite".	Regional user committees will be used to scope the "end user" training deficit and develop cost estimates and an action plan in conjunction with IM&TS and HR representatives. Corporate Services is moving into a "learning organization" mode, and we will ensure that our partners are in on it and will present recommendations to DMC.	Regional Directors of Informatics (all regions)	Draft action plan for March 31, 2000 March 31, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
8. Corporate Services IM&TS in Regions and the NCR work with clients to establish reasonable and effective means for standardizing: 1) Acceptable levels of network performance 2) Firewall Rules 3) Levels of service to small offices, remote locations and ships 4) A mechanism for assessing the evolution of the desktop standard and e-mail 5) A suite of policy statements in the areas identified in section 3.4.1 of this report 6) What services and areas qualify for 24 hour support 7) What services and areas must have no single points of failure 8) Chargeback and support arrangements for program based large scale multi-region IT initiatives 9) IT and WAN/LAN services provided to tenant departments (e.g. NRCan)	Corporate Services IM/TS will develop a workplan to address each issue and table a point by point action plan for each of these at the National Informatics Committee by September 1, 2000	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
9) Corporate Services IM/TS develop an effective and comprehensive needs statement for the WAN, which would include clearly stated performance criteria, reporting requirements based on the needs of IM/TS staff in NCR and the Regions, and penalties for failure to perform according to specified standards and use this as the basis for contracting for the WAN services so as to avoid the many weaknesses identified in the current arrangements.	Telecommunications services will be acquired to meet specified performance and security targets.	Director, Technology Services	Commence April 1, 2000
10) Steps taken by regional Corporate Services IM/TS staff to work towards addressing architecture and firewall inconsistencies be expanded to include NCR staff and clients so that a comprehensive solution that recognizes client needs can be implemented.	Implement and refine current firewall replacement and management plan, working with clients, as part of our on-going management and maintenance of the infrastructure.	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
11) Corporate Services IM/TS and the Communications Directorate work together to identify an orderly and reasonable approach to the use of electronic communications and information sharing. Consultations should include program areas that currently sponsor Web publishing both internally and on the open Internet.	Corporate Services IM/TS will work with DFO Communications to develop a comprehensive plan that will consolidate DFO's WEB presence and ensure that systematic and standardized approaches are established, and that outdated and irrelevant materials are removed.	Director, Planning and Information Management Services / Director Operations Branch, Communications	April 1, 2000
12) The Coast Guard, in cooperation with GTIS and Corporate Services IM/TS, assess the degree to which program needs can be met and savings can be achieved through harmonized acquisition of telecommunications services. Such an assessment is especially desirable given the technical similarities of the soon to be implemented INNAV system to the equipment and links currently operated by Corporate Services IM/TS.	Corporate Services IM/TS will meet with staff from the Coast Guard to identify where harmonized acquisition of telecommunications services would be beneficial. A report on theses discussions will be provided to the National Informatics Committee by September 1, 2000	Director, Technology Services / DG, Technical and Operational Services - CCG	April 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
13) Corporate Services IM/TS advance the Acceptable Use Policy for IT resources so as to provide clarity on what is, and what is not acceptable for DFO employees.	Corporate Services IM/TS will routinely monitor Internet use, as called for in Treasury Board Secretariat policy, and report the findings to the National Informatics Committee quarterly. Further, IM/TS will ensure that action is taken when any unacceptable uses are identified.	Director, Planning & Information Management Services	Completion date: May 31, 2000

REVIEW
DIRECTORATE

DIRECTION GÉNÉRALE
DE L'EXAMEN

Fisheries and Oceans Canada
Pêches et Océans Canada

Canada

EXAMEN DE LA GESTION DES TECHNOLOGIES DE L'INFORMATION

Avril 2000

TABLE DES MATIÈRES

1.0 SOMMAIRE 3

2.0 INTRODUCTION 9

2.1 CONTEXTE 9
2.2 OBJECTIFS ET PORTÉE 10
2.3 MÉTHODOLOGIE 11

3.0 OBSERVATIONS 13

3.1 LES TECHNOLOGIES DE L'INFORMATION SONT ESSENTIELLES 13
3.2 DÉPENSES MINISTÉRIELLES AU TITRE DES TECHNOLOGIES DE L'INFORMATION 15
3.2.1 Dépenses de technologies de l'information 15
3.2.2 Comparaison des dépenses avec celles d'autres ministères et organismes 24
3.3 RÉGIE 28
3.3.1 Rôles et responsabilités 28
3.3.2 Le besoin d'approches consultatives entre clients et fournisseurs 29
3.3.3 Les grands systèmes 30
3.3.4 L'administration du réseau étendu de la DGGIST 31
3.3.5 Le besoin de soutien des TI en dehors des heures normales de travail 34
3.4 LE BESOIN DE POLITIQUES 35
3.4.1 Aspects généraux nécessitant des améliorations 35
3.4.2 Souhaitable ou nécessaire 37
3.4.3 L'évolution de la suite de bureautique standard 38
3.4.4 Internet – « Où puis-je aller aujourd'hui? » 39
3.4.5 Accès à partir de sites éloignés 43
3.5 SÉCURITÉ 44
3.5.1 Évaluation de la menace et des risques 44
3.5.2 Sécurité physique des actifs et de l'information 48
3.5.3 Authentification sécurisée, chiffrement et infrastructure de clés publiques (ICP) 49
3.5.6 La sécurité et l'Internet - les systèmes coupe-feu 50
3.6.7 Élimination des points de défaillance des systèmes essentiels 51
3.6 COMMUNICATIONS 52
3.6.1 Canaux de communications 52
3.6.2 La publication Web 52
3.7 FORMATION 54
3.7.1 Déficit de formation 54

4.0 RECOMMANDATIONS 56

REMERCIEMENTS 58

5.0. PLAN D'ACTION DE GESTION 59

1.0 SOMMAIRE

CONTEXTE

Les technologies sont clairement présentes dans la conduite des activités du MPO. Le sondage du personnel ministériel réalisé dans le cadre de cet examen indique que 97 % des employés ont accès à un ordinateur ou en utilisent un dans leurs activités quotidiennes.

Employés ministériels	%
Qui ont accès à un ordinateur dans leurs activités de travail régulières	97
Qui ont besoin des technologies de l'information pour s'acquitter de leurs responsabilités ministérielles	81
Qui sont soutenus par les technologies de l'information pour s'acquitter de leurs responsabilités ministérielles	69
Qui sont soutenus par les technologies de l'information dans leur travail avec d'autres employés du Ministère	72
Qui utilisent de grandes applications personnalisées	30
Qui estiment que leur système actuel répond entièrement à leurs besoins	88
Qui estiment que leur système actuel sera suffisant pour les 12 prochains mois	74
Qui ont utilisé l'Intranet du MPO au cours du dernier mois	72
Qui ont utilisé l'Internet au cours du dernier mois	82
Qui utilisent les services du Bureau d'assistance et les trouvent bons, très bons ou excellents	85
Qui n'utilisent jamais les services du Bureau d'assistance	24

La conclusion la plus importante de cet examen est que le MPO doit gérer ses technologies de l'information en utilisant des modèles de planification opérationnelle clairs qui relient les circonstances actuelles aux objectifs futurs, font largement appel à la participation des utilisateurs et évaluent clairement les coûts et les répercussions techniques.

Au MPO, les technologies de l'information (TI) englobent tous les systèmes informatiques ministériels, y compris les matériels et les logiciels, ainsi que les réseaux qui les relient. Les actifs informatiques comprennent plus de 8 000 ordinateurs personnels, ainsi que 18 grands systèmes personnalisés. Ces grands systèmes appuient différentes activités, depuis l'enregistrement national des infractions aux règlements sur les pêches jusqu'au suivi du parcours des navires en mer. Un total de 94 ordinateurs sont spécialement utilisés comme « routeurs » pour l'exploitation du réseau étendu et des réseaux locaux (RE/RL). Les technologies permettent aux employés du Ministère d'effectuer une foule de fonctions, dont le traitement de texte, les analyses techniques, l'enregistrement et la transmission de données, la recherche d'information sur l'Internet, etc.

Cet examen avait pour objet d'évaluer la gestion des technologies de l'information au MPO. L'examen, de portée nationale, portait sur les aspects suivants : les budgets d'immobilisations et d'exploitation consacrés aux technologies de l'information; les processus de gestion régissant la planification et l'acquisition des technologies de l'information; la qualité des services fournis; une

analyse des tendances récentes en matière de sécurité de l'utilisation des TI, et l'utilisation de l'Internet.

Il importe de souligner que plusieurs avancées importantes dans la gestion des technologies de l'information ont eu lieu au Ministère au cours de la dernière décennie. En effet, en 1995, la Direction générale de la gestion de l'information et des services de la technologie (DGGIST) des Services intégrés a entrepris de développer une architecture informatique standard pour le MPO. La Direction générale a invité le personnel et les clients de la DGGIST de toutes les régions et de la RCN à y participer. Cette initiative d'architecture informatique (qui était financée par le Secrétariat du Conseil du Trésor et qui a par la suite reçu un prix du SCT) a amélioré l'efficacité technique des réseaux et fait en sorte qu'ils puissent fonctionner comme un ensemble intégré. Cette initiative d'architecture comportait l'harmonisation complète des matériels et des logiciels.

SOMMAIRE DES CONSTATATIONS ET CONCLUSIONS

Les dépenses du MPO au titre des TI constituent un élément important des dépenses totales. En 1997-1998, les dépenses de TI s'établissaient à 66,9 millions $, ce qui correspond à 6,1 % des dépenses totales. Ces dépenses se répartissaient en six catégories :

Catégorie	Dépenses (en millions)	Pourcentage des dépenses totales de TI
Matériels	22,7 $	34 %
Services de consultation	19,6 $	29 %
Salaires de la DGGIST (à l'exclusion de la bibliothèque et des dossiers centraux)	12,7 $	19 %
Télécommunications (non vocales)	8,9 $	13 %
Logiciels	2,9 $	4 %
Fournitures	0,1 $	1 %

Ce montant correspond à une dépense annuelle de 6 658 $ par employé à temps plein (ETP). Cette somme ne comprend pas les salaires des employés des programmes qui consacrent tout leur temps ou une partie importante de leur temps à la gestion des TI.

Nous avons également comparé les dépenses de TI du MPO en 1997-1998 avec celles d'autres ministères ayant des mandats semblables. Le MPO dépense plus que Santé Canada (5 400 $) ou qu'Agriculture et Agro-alimentaire Canada (6 000 $), mais moins que Ressources naturelles Canada (9 500 $) ou qu'Environnement Canada (9 700 $). En réponse à une demande de la haute direction (faite pendant que le Comité ministériel de l'examen discutait du rapport intérimaire), nous avons également établi quelques comparaisons plus globales avec les dépenses des entreprises nord-américaines et des gouvernements des États-Unis aux niveaux fédéral, étatique et local. Ces données ont révélé qu'il existait d'importantes variations et que les dépenses de TI augmentaient considérablement (de l'ordre de 16 fois plus) entre les organisations ayant un

engagement modéré à l'égard des solutions de TI et celles qui les mettent en œuvre de façon plus soutenue.

Les dépenses totales de TI, soit 6 658 $ par ETP, équivalent à 2 818 $ (42 %) pour la DGGIST et à 3 840 $ (58 %) à l'intérieur des programmes. À la DGGIST, la dépense la plus importante est au titre des salaires, suivis par les matériels, les consultants et les communications de données. Ces dépenses salariales élevées reflètent l'important contingent de ressources spécialisées qui sont rattachées à la DGGIST. Dans le secteur des programmes, où bon nombre des grands logiciels personnalisés sont développés, la dépense la plus importante est au titre des consultants (42 %). Étant donné cette importante dépense de services de consultation, l'on se demande pourquoi les gestionnaires de TI des programmes n'utilisent pas davantage les ressources expertes internes de la DGGIST, ce qui permettrait de réaliser d'importantes économies de coûts. Il semblerait que ces ressources internes ne sont pas davantage exploitées à cause du processus décisionnel extrêmement décentralisé et non coordonné qui est actuellement utilisé pour gérer les TI. En effet, on a parfois développé des solutions spécifiques, différentes et redondantes pour résoudre des problèmes qui se retrouvent dans plusieurs secteurs ou régions. Il faut mieux définir les rôles et les responsabilités. L'exemple suivant illustre ce sujet de préoccupation.

L'actuel fournisseur de services de télécommunications du Ministère a indiqué que des services semblables sont actuellement achetés séparément par la Garde côtière canadienne (GCC) et par la DGGIST. Il a également indiqué qu'il serait possible de réaliser des économies si tous les circuits et les services étaient achetés de façon intégrée. L'équipe d'examen recommande donc que la Garde côtière canadienne, en collaboration avec la DGGIST des Services intégrés et les SGTI, évalue les économies qui pourraient être réalisées par l'acquisition harmonisée de ces services de réseau. De façon plus générale, ce genre de chevauchement pourrait être évité s'il y avait un processus décisionnel plus clair, faisant en sorte que tous les investissements de TI soient entièrement évalués, à la fois du point de vue de la satisfaction des besoins des programmes et de la conformité aux normes et à l'architecture ministérielles. Nous recommandons que la haute direction définisse et précise les rôles et les responsabilités afférents à la gestion des TI.

Plusieurs investissements « ponctuels » dans les TI ont été effectués au cours des trois dernières années. Chacun de ces investissements a procuré des avantages mesurables correspondant aux objectifs de l'investissement. Ce qui n'a pas été prévu, c'est la fourniture de fonds stables, sur une base continue et à long terme, pour assurer le fonctionnement des activités de base et leur évolution en fonction des besoins. Ces fonctionnalités de base comprendraient vraisemblablement le réseau étendu et les réseaux locaux, les systèmes d'exploitation, la suite de logiciels de bureautique, le Bureau d'assistance, et la désignation de gestionnaires de portefeuille de TI. Elles seraient administrées par la DGGIST, aux Services intégrés et dans les régions.

De tous les éléments de ces fonctionnalités de base, le réseau (y compris le courrier électronique, les logiciels de bureautique et l'aide aux utilisateurs) est la composante la plus importante, essentielle à la mission ministérielle. Le courrier électronique, le partage de fichiers et les systèmes intégrés de gestion des finances et du personnel ne peuvent fonctionner que si le réseau fonctionne correctement. L'équipe d'examen a établi la topologie détaillée du fonctionnement du réseau et découvert un grave manque d'uniformité dans son administration. Un réseau étendu est

administré depuis la RCN, tandis que plusieurs RL sont administrés dans les régions ainsi que dans la RCN. Chacun de ces réseaux est exploité et administré de façon différente dans chaque région. Le financement de base aurait l'avantage d'éliminer ce manque d'uniformité au chapitre de l'administration et du niveau de service fourni aux utilisateurs. Nous avons également appris que d'importantes économies pourraient être réalisées si le MPO mettait en place une architecture ministérielle unique pour le réseau étendu. Le financement de base éliminerait aussi l'actuel système de facturation interne, qui est administré de façon inégale, pour les services de gestion de RL dans la RCN et dans certaines régions.

Pour que le concept des fonctionnalités de base fonctionne, il faut définir clairement ce qui est compris et ce qui ne l'est pas, et réaliser une évaluation explicite et vérifiable du niveau de financement qui devrait être fourni. L'équipe d'examen recommande qu'un financement de base soit fourni pour le réseau, l'environnement de bureautique (postes de travail), le Bureau d'assistance et la gestion de portefeuilles.

Il est nécessaire de préciser les responsabilités et le financement de base pour renforcer la gestion des technologies de l'information. Ce renforcement ne peut se faire que si les responsables de la gestion des TI à la DGGIST et dans le secteur des programmes font un effort plus concerté pour se consulter, apprendre et collaborer. Ils doivent aussi faire un effort plus concerté pour consulter et écouter les utilisateurs des technologies de l'information.

Le concept de « gestionnaire de portefeuille » qui est maintenant utilisé dans la RCN et dans plusieurs régions est une approche qui semble bien fonctionner pour promouvoir la consultation et la coopération. Selon cette approche, la DGGIST désigne une personne qui deviendra un expert et assurera la continuité de la satisfaction des besoins de TI d'un secteur de programme particulier. Là où ces postes existent et où les liens avec les secteurs de programme sont maintenus, il s'agit clairement d'une « pratique optimale ».

Nous avons également examiné l'état des mécanismes de consultation entre les fournisseurs de TI et les utilisateurs. Il existe actuellement des mécanismes de consultation entre les clients et les fournisseurs dans divers secteurs et régions, mais l'on ne peut discerner aucun schéma définissable. Dans les régions, nous avons trouvé des comités qui avaient été mis sur pied pour des projets précis. D'autres étaient organisés sur une base multisectorielle ou entre un secteur et la DGGIST pour répondre aux besoins d'un programme en particulier. Ces comités sont surtout concentrés dans la région du Pacifique, où les ressources de TI sont généralement rattachées à des programmes. Au niveau national, il n'existait pas de structure de comités clients-fournisseurs au moment de cet examen. Au début de 1999, les Services intégrés ont pris l'initiative d'organiser un Comité directeur de l'informatique (CDI) à l'échelle nationale. Ce comité devrait devenir un forum important pour donner suite à bon nombre des initiatives recommandées dans cet examen.

Un exemple révélateur du besoin d'un programme de consultation beaucoup mieux coordonné est le déploiement de la suite de bureautique Microsoft Office 97, qui remplace maintenant partiellement la suite Office 4.3. Nous avons analysé les processus de gestion qui ont été appliqués pour justifier la décision d'adopter la nouvelle version du logiciel et examiné dans quelle mesure les utilisateurs avaient été consultés. Or, la nouvelle version du logiciel a été achetée en tant que

norme ministérielle nationale, alors qu'aucun dossier justificatif n'avait été préparé pour montrer les avantages supplémentaires et que les données d'inventaire indiquaient qu'un nombre substantiel d'utilisateurs seraient dans l'impossibilité d'adopter la nouvelle norme. En outre, les clients n'ont pas été consultés sur le besoin de capacité accrue qu'entraînerait l'introduction d'Office 97. Le coût de la licence d'exploitation d'Office 97 s'établissait à environ 700 000 $. Cependant, l'équipe d'examen a déterminé que l'implantation du logiciel a suscité un besoin de formation qui a coûté environ 900 000 $ de plus. L'équipe d'examen recommande donc que les futures mises à niveau généralisées soient appuyées par un dossier justificatif complet faisant appel à la participation des utilisateurs et incorporant le coût des mises à niveau matérielles et de la formation. L'équipe d'examen recommande également que la DGGIST des Services intégrés élabore un mécanisme pour répondre aux besoins de formation qui ont été créés par l'introduction récente de nouveaux logiciels.

L'équipe d'examen a évalué dans quelle mesure la gestion des TI se conforme actuellement aux normes et aux politiques administratives. La plupart du temps, ces normes et politiques se rapportent aux questions « qui fait quoi? » et « comment? ». Les exemples suivants illustrent l'absence actuelle de politiques et de normes et l'actuel degré de conformité ou de non-conformité à ces normes, quand elles existent.

Le MPO a conclu un contrat avec les Services gouvernementaux de télécommunications et d'informatique (SGTI) de Travaux publics et Services gouvernementaux Canada (TPSGC) pour la gestion du réseau étendu de la DGGIST. Les SGTI ont quant à eux confié la gestion du système à une entreprise locale, NUVO Networks. Nous avons examiné l'accord détaillé sur les niveaux de service (ANS) que le MPO a négocié avec les SGTI et constaté que les rapports et la gestion de la « largeur de bande » (le niveau de trafic dans le système) n'étaient pas conformes aux normes de performance stipulées dans le contrat. De plus, les SGTI, qui sont chargés de faire des recommandations sur l'architecture du réseau étendu, n'en ont rien fait. Étant donné ce non-respect des normes, nous recommandons que la DGGIST des Services intégrés prépare un énoncé complet des besoins pour la performance du réseau étendu. Des mesures correctives devraient être prises si les niveaux de service ne sont pas respectés.

La gestion de l'Internet est un autre aspect important où nous avons constaté que les niveaux de service présentaient de graves lacunes. L'interface ministérielle avec l'Internet est gérée par six « coupe-feu » dans la RCN et les régions. Ces systèmes sont actuellement gérés de façon inégale et en l'absence de toute norme. Le réseau étendu et les réseaux locaux sont configurés de telle façon que le coupe-feu le moins permissif établit le risque pour l'ensemble du système. Nous avons également constaté que l'architecture du système de courrier électronique est très vulnérable aux risques associés à l'Internet. Étant donné la vulnérabilité apparente du système, nous recommandons que la DGGIST des Services intégrés réalise une évaluation de la menace et des risques de l'accès Internet et de la configuration des systèmes de courrier électronique pour évaluer les niveaux de risque actuels.

Nous avons découvert de nombreux autres aspects qui présentent un manque d'uniformité et pourraient bénéficier de normes et de politiques cohérentes. Nous recommandons que la DGGIST dans les régions et dans la RCN collabore avec les clients pour établir des moyens raisonnables et

efficaces de normaliser les éléments suivants : les règles afférentes aux systèmes coupe-feu, les niveaux de service, les services devant faire l'objet d'un soutien permanent (24 heures sur 24), les services qui ne doivent absolument pas connaître de défaillance, et les services fournis aux sites éloignés, y compris les navires.

Nous avons étudié les systèmes de grande taille dans la RCN et dans la région des Maritimes pour déterminer comment ces systèmes sont gérés depuis leur conception jusqu'à leur mise en œuvre. Les systèmes de grande taille se définissent comme les systèmes qui coûtent plus de 500 000 $, qui sont fournis à plus de 100 employés ou qui sont mis en œuvre dans de multiples sites. Au moins deux des systèmes examinés, le Departmental Violations Information System et le Habitat Referrals Tracking System, sont passés d'un coût prévu de moins de 100 000 $ à un coût de livraison de plus de 1 million $. Dans les cas où il n'y avait pas de plans détaillés, les coûts étaient plus élevés que prévu et, dans certains cas, les produits livrables n'avaient pas été fournis pendant l'année au cours de laquelle ils étaient attendus. Dans l'ensemble, nous avons constaté que les systèmes qui avaient été développés par des équipes de projet spécifiques, comprenant du personnel de la DGGIST des Services intégrés et des régions, ainsi que des experts des programmes et des consultants, étaient ceux qui fonctionnaient le mieux. La région des Maritimes et la région Laurentienne ont développé un système de planification efficace pour les systèmes de grande taille. Nous recommandons donc que le MPO exige que tous les grands systèmes de TI soient évalués à l'aide d'un outil complet de planification et d'évaluation de projet.

Dans le cadre de son mandat, l'équipe d'examen s'est également penchée sur les questions relatives à l'utilisation actuelle des TI et à la façon dont cette utilisation se répercute sur la sécurité de l'information, sur ce qui constitue une « utilisation acceptable » de l'Internet par les employés du MPO, et sur les communications ministérielles.

Le sondage des utilisateurs a révélé que, de tous les services de TI partagés, c'est le courrier électronique qui est le plus apprécié. La Garde côtière canadienne a récemment commandé la réalisation d'une étude approfondie de la sécurité, qui a déterminé que l'actuel système de courrier électronique pouvait être intercepté et trafiqué. L'équipe d'examen n'a trouvé aucune politique stipulant que les utilisateurs devaient être informés du niveau de sécurité de l'information qui peut être transmise par courrier électronique. Nous recommandons donc à la DGGIST des Services intégrés d'informer les utilisateurs du niveau de sécurité du système actuel du MPO et des types de renseignements qui peuvent être transmis ou non.

Actuellement, tous les utilisateurs du MPO ont accès à l'Internet. Le nombre moyen de réponses ou « consultations » Internet par jour (par employé à temps plein) est d'environ 28 dans la RCN, les Maritimes, à Terre-Neuve et dans la région du Centre et de l'Arctique. Cette moyenne s'établit à environ 42 dans la région Laurentienne, et à 67 consultations par jour dans la région du Pacifique. Nous avons déterminé qu'environ 10 % du trafic Internet actuel du MPO se rapporte à des sujets qui n'ont aucun lien apparent avec le travail (soit les annonces, les nouvelles, les sports et le sexe, etc.). Le MPO ne vérifie pas les sites Internet qui sont consultés. Nous recommandons donc au MPO d'établir une « Politique d'utilisation acceptable » pour préciser ce qui est acceptable et ce qui ne l'est pas pour les employés ministériels qui utilisent les ressources de TI.

Enfin, l'équipe d'examen a également examiné brièvement comment les TI ont facilité les communications internes et externes du MPO. En ce qui concerne les communications internes, le sondage des utilisateurs a révélé quelques signes de « surcharge » d'information. Il n'existe aucune politique indiquant quels types d'informations se prêtent à la diffusion électronique. L'absence d'orientations claires vaut aussi pour la publication sur l'Internet. L'équipe d'examen a constaté que le MPO dépensait environ 2 millions $ chaque année au titre de la publication Internet. Il n'existe aucun mécanisme de vérification qui fasse en sorte que ce qui est publié est valable et contribue à la réalisation des objectifs ministériels. La Direction générale des communications est responsable de l'application des normes du Ministère et du Conseil du Trésor, mais ses responsables ont indiqué qu'ils n'exercent aucune surveillance. Nous recommandons donc à la DGGIST des Services intégrés de collaborer avec la Direction générale des communications pour identifier une approche ordonnée et raisonnable en ce qui concerne l'utilisation des communications électroniques.

2.0 INTRODUCTION

2.1 CONTEXTE

Les technologies de l'information sont maintenant des outils essentiels à la réalisation des programmes ministériels. Ces technologies comprennent non seulement les ordinateurs de grande et de petite capacité, mais aussi les systèmes d'interconnexion électroniques qui relient les dispositifs de TI. Les ordinateurs eux-mêmes ont évolué, passant d'outils de recherche tournant sur de gros ordinateurs de la taille d'une pièce et de « machines à écrire dotées de mémoire » à une infrastructure interconnectée qui nous est aussi indispensable que nos immeubles et nos téléphones. Lors du sondage téléphonique réalisé en juin 1998 par PriceWaterhouseCoopers pour cet examen, 97,8 % des répondants ont indiqué qu'ils utilisent un ordinateur dans leurs activités de travail *régulières*. De plus, 94 % des répondants ont indiqué que les ordinateurs leur sont essentiels pour s'acquitter de leurs responsabilités ministérielles.

À l'origine, les ordinateurs étaient simplement des outils individuels, utilisés par des personnes, des programmes et des groupes particuliers. Quand leur utilisation est devenue plus généralisée, de petits groupes se sont organisés pour former des réseaux. Au début, c'étaient des « groupes de travail » locaux, puis des regroupements de plus en plus importants, et maintenant, notre actuel système national a des liens continus avec tous les bureaux et les navires, sauf les plus éloignés (qui sont desservis par l'accès commuté à distance, ainsi que par des liaisons cellulaires et par satellite).

La croissance de l'architecture informatique du MPO s'est d'abord faite à l'intérieur des groupes de travail ministériels. Certains groupes, comme la Direction des ports pour petites embarcations et la Division de l'inspection du poisson (qui a depuis quitté le Ministère), ont même établi un réseau national indépendant; d'autres ont installé des liaisons internes par « secteur » et d'autres encore, en particulier le secteur des Sciences, ont commencé à utiliser l'Internet pour collaborer avec des collègues à l'intérieur et à l'extérieur du MPO. La Garde côtière canadienne avait établi des liaisons électroniques interurbaines, directement et par l'entremise de Transports Canada, pour connecter des bureaux clés partout au Canada bien avant sa fusion avec le MPO. Même si des

mesures ont été prises pour faire en sorte que le courrier électronique et les applications de bureautique de la Garde côtière fonctionnent sur le réseau étendu (RE) géré par la DGGIST, certains éléments techniques des deux systèmes demeurent très semblables et sont administrés séparément.

À la suite d'une série d'études sur la Direction générale de la gestion de l'information et des services de la technologie (DGGIST) réalisées par Price Waterhouse entre 1992 et 1994, et après les travaux considérables effectués par la DGGIST au sein du MPO, une « architecture » standard a émergé. Grâce à la fourniture de fonds ponctuels ciblés, un système uniforme plus intégré a été mis en œuvre. Le document sur l'architecture informatique du MPO et les initiatives d'infrastructure subséquentes ont considérablement amélioré l'interopérabilité technique du réseau et de ses systèmes. Ce processus a été efficace en ce qu'il a permis aux réseaux gérés par la DGGIST et la Garde côtière de fonctionner comme un ensemble intégré. Certains problèmes touchant la planification, le financement et la gestion des actifs informatiques dans l'ensemble du Ministère doivent cependant être résolus pour que ces réseaux fonctionnent efficacement et répondent aux besoins ministériels de façon économique et rentable.

Bien que nous soyons maintenant physiquement interconnectés, la gestion des TI diffère encore considérablement d'un secteur à un autre, et même à l'intérieur d'une région ou d'un secteur. Il existe des tensions intersectorielles et l'on a parfois développé des solutions spécifiques, différentes et redondantes pour résoudre des problèmes qui se retrouvent dans plusieurs secteurs ou régions, sans s'occuper des avantages qu'une coordination plus serrée aurait pu procurer.

La gestion des TI est importante car, au cours des trois derniers exercices, le MPO a dépensé environ 66,9 millions $ par année (soit 6,1 % des dépenses totales) pour les TI (selon une analyse des dépenses par article d'exécution). Cela revient à environ 6 658 $ par employé par année. Bien qu'il n'existe pas de données directement comparables provenant d'autres ministères fédéraux ayant une mission semblable, nous avons réalisé une comparaison des dépenses non salariales. Sur la base de ces données, les dépenses du MPO correspondent à celles d'autres ministères fédéraux semblables (c.-à-d. que les dépenses sont inférieures à celles de Ressources naturelles et d'Environnement Canada, mais supérieures à celles d'Agriculture et Agro-alimentaire Canada et de Santé Canada). La section 3.2.2 de ce rapport contient un tableau de ces dépenses.

2.2 OBJECTIFS ET PORTÉE

Nous avons évalué la gestion des TI des points de vue suivants :

- Une évaluation générale des budgets de fonctionnement et d'immobilisations et des ETP participant directement à la gestion des TI.
- La mise en œuvre d'une interface appropriée pour les politiques et la planification entre tous les gestionnaires de TI du Ministère, et entre ces gestionnaires et leurs clients respectifs.
- La nature et l'efficacité des outils de planification stratégique utilisés dans tous les secteurs du MPO qui régissent l'acquisition et la gestion des TI.
- La capacité du Ministère à encourager et à promouvoir l'utilisation des technologies pour soutenir et améliorer :

1. L'exécution des programmes destinés aux clients
2. La productivité du personnel
3. Les communications internes
4. La fourniture aux gestionnaires d'information sur les résultats et la situation financière des programmes.

- La conformité aux politiques du Conseil du Trésor.

Nous avons examiné un échantillon d'investissements récents pour déterminer s'ils avaient été évalués et exécutés dans un cadre de gestion de l'information. Ces exemples étaient basés sur les systèmes de grande taille utilisés dans tous les secteurs pertinents. Les investissements récents dans les matériels, les logiciels et les services comprennent : Abacus, Peoplesoft, Windows NT Server, l'adoption d'Office 97, Microsoft Exchange/Outlook, le Habitat Referrals Tracking System, le Departmental Violations System et la mise en œuvre d'une nouvelle norme matérielle pour postes de travail. Une analyse sommaire des stratégies et des consultations qui ont précédé ces acquisitions a été faite. Il était important d'identifier si des projections relatives aux économies de coûts et à d'autres avantages, comme la réduction des interruptions et l'augmentation de la fiabilité, avaient été faites avant la mise en œuvre de ces changements informatiques, et si les avantages prévus avaient été réalisés.

La portée de cet examen englobait la gestion des matériels, des logiciels personnalisés et commerciaux, des outils d'interconnexion et de communication réseau, des installations fixes et des matériels portables. Étaient également comprises les TI qui sont fournies au Ministère sur une base de crédit-bail, de location ou de licence (à l'exclusion des communications téléphoniques vocales locales et interurbaines). Un volet clé de cet examen visait l'identification et l'évaluation des mécanismes de livraison et de soutien.

L'équipe d'examen a coordonné ses travaux avec l'examen de la restructuration des Services intégrés et le projet d'options de régie, et tenu compte de tous les travaux d'inventaire pertinents qui avaient déjà été réalisés. Elle a également utilisé, lorsque cela était pertinent, des informations tirées d'études récentes portant sur la gestion des TI (par exemple, Peoplesoft et Abacus).

2.3 MÉTHODOLOGIE

L'examen s'est déroulé de février à décembre 1998. Des études spécifiques ont été réalisées, certaines par des membres de la Direction générale de l'examen du MPO, d'autres par des consultants travaillant sur leur supervision. Nous avons déployé des efforts considérables pour travailler en étroite collaboration avec des membres clés du personnel ministériel à mesure que l'examen progressait.

Nous avons suivi trois filières d'enquête majeures et cinq filières mineures. Seulement une d'entre elles, le sondage des utilisateurs, sera diffusée dans un rapport distinct. De plus, toutes les études ministérielles majeures portant sur les TI, les réseaux, la fonction informatique et la sécurité des TI depuis 1991 ont été évaluées du point de vue de leur actualité et de leur pertinence pour les objectifs de la présente étude.

Les trois éléments majeurs ont été le sondage des utilisateurs, l'analyse et la comparaison des dépenses ministérielles de TI et l'examen du réseau étendu, de l'Internet et de la sécurité.

1) Le sondage du personnel ministériel s'est fait par téléphone au cours de l'été 1998. Ce sondage présente les résultats par région et par secteur, avec un taux d'exactitude de 90 %. Les résultats du sondage ont été comparés à ceux d'autres sondages semblables réalisés dans d'autres organisations. Les principaux aspects de réalisations (pratiques optimales) et les aspects nécessitant une attention ont été identifiés.

2) Les dépenses ministérielles des trois derniers exercices (1995-1996, 1996-1997 et 1997-1998) ont été analysées et comparées. Les articles de dépenses reliés aux TI ont été identifiés et mis en correspondance avec les systèmes de l'ancien MPO et de la Garde côtière au cours de la période de trois ans. Toutes les dépenses du Ministère ont été triées par région et par secteur, les dépenses de l'ancien MPO étant consignées par secteur d'activité et celles de la Garde côtière, par centre de responsabilité. Les dépenses ont été illustrées au moyen de graphes et leurs tendances ont été identifiées, et des comparaisons interrégionales et intersectorielles ont été faites. Les montants ont ensuite été comparés aux équivalents temps plein (ETP) (comme on en trouve dans le Système de gestion des salaires) et aux dépenses totales (par région, par secteur et à l'échelle nationale). L'analyse la plus importante a consisté à examiner les comparaisons interrégionales, intersectorielles et inter-exercice. Les dépenses ministérielles ont ensuite été comparées aux dépenses de trois autres ministères de « ressources naturelles » et de Santé Canada. Des comparaisons plus larges avec des entreprises nord-américaines et des gouvernements américains (fédéral, d'État et locaux) ont également été faites. Bien que ces comparaisons soient quelque peu éloignées de la situation du MPO, elles aident à déterminer si le Ministère est dans les normes, par rapport à un contexte plus large, et elles ont été demandées par la haute direction lors d'une réunion portant sur le rapport intérimaire.

3) La troisième étude majeure portait sur les éléments « de base » du réseau, et incluait le réseau étendu qui relie tous les grands centres ministériels, sa capacité et l'utilisation de cette capacité, mesurée par les rapports quotidiens exigés par le Ministère. Cette étude examinait également les caractéristiques du trafic Internet à chacun des six systèmes coupe-feu du Ministère (les dispositifs qui s'interfacent entre le réseau du MPO et l'Internet). Cette étude avait pour objet d'évaluer le volume et la nature du trafic Internet et la mesure dans laquelle l'utilisation de l'Internet est un facteur coût pour l'infrastructure ministérielle. Le dernier volet de cette étude était une évaluation des questions de sécurité. Ce volet a mis l'accent sur la mise en œuvre de mesures de sécurité raisonnables et nécessaires pour l'information protégée, sur la sécurité des équipements des réseaux locaux (RL) et du réseau étendu (RE) et sur la protection contre les accès non autorisés de n'importe quelle origine (y compris l'Internet).

Les cinq volets mineurs étaient les suivants :

1) Une analyse des politiques ministérielles de gestion des TI, des structures de comités et des documents de planification, afin d'évaluer leur portée et leur efficacité, ainsi que la mesure

dans laquelle ils tiennent compte des besoins des programmes du MPO et font appel à la participation des clients;

2) Une analyse de la gestion des grands systèmes logiciels personnalisés qui fonctionnent au niveau national ou régional, afin d'évaluer le dossier justificatif qui a été présenté, ainsi que les processus d'acquisition et de développement utilisés et la mesure dans laquelle le produit correspondait aux objectifs et aux estimations de coûts initiales;

3) Une analyse des politiques et des pratiques de gestion actuelles entourant l'accès à distance aux systèmes informatiques du MPO, afin d'évaluer la conformité aux politiques, les coûts et la mesure dans laquelle le MPO a mis en œuvre des possibilités de télétravail;

4) Une analyse des processus de gestion utilisés pour la récente décision de changer de suite de bureautique standard (mise à niveau de Microsoft Office 4.3 à Microsoft Office 97), changement qui a affecté tous les utilisateurs du Ministère. Cette analyse visait à identifier les processus de gestion implicites et explicites qui ont été utilisés pour identifier le besoin opérationnel et le produit spécifique, ainsi que la mesure dans laquelle les utilisateurs ont participé au processus décisionnel, et les améliorations opérationnelles que ce changement a procurées aux utilisateurs;

5) Une analyse de la gestion de la publication Web sur l'Internet et l'Intranet du Ministère, afin de déterminer dans quelle mesure ce nouveau moyen de communications avait été assujetti aux mêmes normes, contraintes et considérations que les publications imprimées, et afin d'en évaluer les coûts et, lorsque c'était possible, l'efficacité.

3.0 OBSERVATIONS

3.1 LES TECHNOLOGIES DE L'INFORMATION SONT ESSENTIELLES

Étant donné que les scientifiques du MPO utilisent les ordinateurs depuis très longtemps et que le Ministère a exploité très tôt des systèmes exclusifs pour des fonctions de bureau comme la correspondance ministérielle, on peut dire que les examens et les évaluations de l'utilisation ministérielle des TI sont aussi vieux que les technologies elles-mêmes. Le présent examen n'a tenu compte que des études les plus récentes sur les TI, soit celles qui ont été réalisées depuis 1991. Presque toutes les études récentes recommandaient un niveau plus soutenu d'organisation et d'intégration dans l'utilisation des ordinateurs et un niveau de soutien accru des programmes ministériels par ce qu'il est maintenant généralement convenu d'appeler les TI.

Bien que toutes les régions et tous les secteurs fassent des dépenses de TI, 56 % des dépenses de TI pour l'exercice 1997-1998 ont été faites par les Services intégrés (42 % des dépenses ministérielles ont été effectuées par la composante DGGIST des Services intégrés.) Le deuxième secteur en importance était la Garde côtière canadienne, avec des dépenses de TI correspondant à 25 % du total ministériel. Le présent examen s'est penché sur les dépenses de tous les secteurs et les régions, mais plus attentivement sur les dépenses de la DGGIST, qui est non seulement le secteur ayant les dépenses les plus élevées, mais aussi le groupe qui assume les responsabilités de base

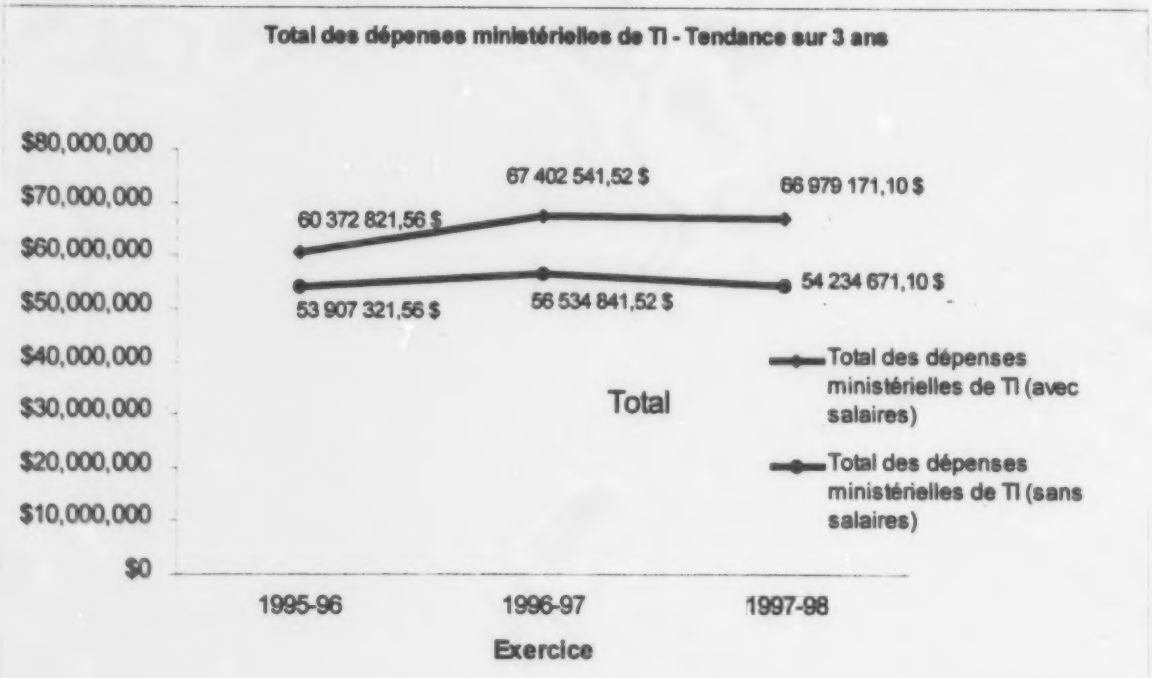
pour la gestion des questions reliées aux TI au MPO. Les autres sections des Services intégrés qui ont d'importantes dépenses de TI, soit Abacus et Peoplesoft, ont déjà fait l'objet d'un examen détaillé et n'ont donc pas été évaluées en détail dans le cadre du présent examen.

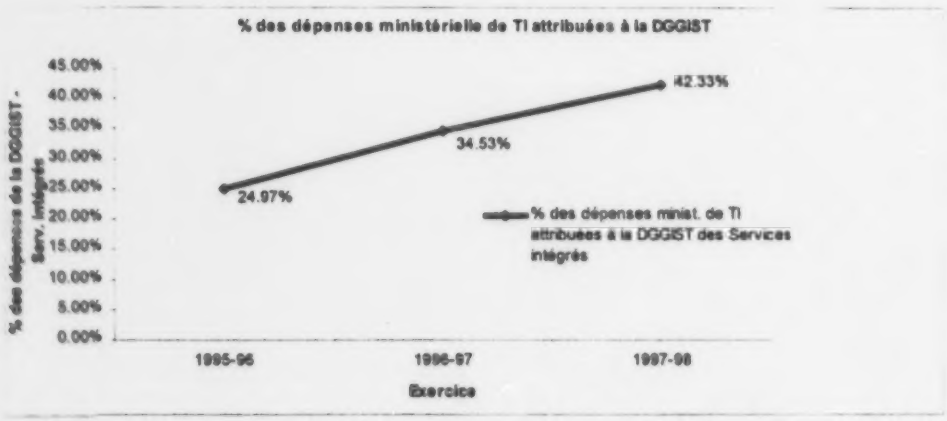
L'interconnexion d'ordinateurs (qui peuvent partager des fichiers et du courrier électronique qui sont compatibles) est la « valeur ajoutée » la plus importante pour l'ensemble du Ministère. Bien que les différents ordinateurs qui exploitent des systèmes spécialisés puissent être essentiels à des éléments de programme précis ou même à des programmes entiers, les avantages d'intercommunication du réseau fonctionnant comme un tout font du réseau l'actif de TI qui est peut-être le plus essentiel au Ministère. Dans les diverses études qui sous-tendent ce rapport, le réseau est clairement essentiel à l'exécution des programmes. Le courrier électronique (courriel), le partage de fichiers et les systèmes intégrés de gestion des finances et du personnel ne peuvent fonctionner que si le réseau fonctionne correctement. Le réseau est aussi essentiel et aussi fondamental que les immeubles dans lesquels nous travaillons et les mécanismes que nous utilisons pour assurer la prestation de nos programmes.

L'équipe d'examen a relevé des inégalités importantes en ce qui a trait à l'administration du réseau, aux niveaux de service et à la facturation interne, au soutien des utilisateurs, à la participation des clients et à la mise en œuvre de la suite de bureautique standard. La suite de bureautique standard et le courriel constituent les deux normes logicielles nationales qui soutiennent les communications entre toutes les parties du MPO. Le courriel est bien intégré et fonctionne généralement de façon ordonnée et fiable. Un réseau étendu (RE) est administré depuis la Région de la capitale nationale (RCN) et plusieurs RL sont administrés au niveau régional (ainsi que dans la RCN). Chacun de ces éléments est exploité et administré de façon différente dans chaque région. Dans certaines régions, il y a du financement de base pour la GI/ST et, dans d'autres, il y a un système de facturation interne qui varie considérablement sur le plan de la quantité et de l'étendue des services qui y sont reliés.

3.2 DÉPENSES MINISTÉRIELLES AU TITRE DES TECHNOLOGIES DE L'INFORMATION

3.2.1 Dépenses de technologies de l'information





Au cours de ces trois exercices, le total ministériel est demeuré relativement stable, mais la proportion des dépenses attribuées à la DGGIST est passée de 25 % à 42 %, ce qui reflète, en partie, les dépenses spéciales « d'infrastructure » faites en 1997-1998 ainsi que l'expansion des « accords sur les niveaux de service » qui transfèrent des fonds des programmes à la DGGIST.

Le tableau suivant illustre les dépenses ministérielles de TI par ETP.

Tableau 3.2.1.1 Dépenses ministérielles de TI par ETP (1997-1998)

Élément	Dépenses
Ensemble du MPO	6 658 $
Dépenses extérieures à la DGGIST	3 840 $
Dépenses de la DGGIST	2 818 $

Tableau 3.2.1.2 Facturation interne de la DGGIST par région en 1997-1998

Région	Facturation interne par ETP
Terre-Neuve	0 $
Maritimes	1 050 $
Laurentienne	0 $
RCN	1 000 $
Centre et Arctique	0 $
Pacifique	0 $

Dans leur ensemble, les deux tableaux précédents confirment que le système de facturation interne pour les services de RL est inégal et que le montant facturé ne présente aucun lien évident avec les dépenses réelles des groupes de la DGGIST dans les différentes régions ou dans la RCN.

Tableau 3.2.1.3 Analyse des dépenses de TI par ETP ministériel en 1997-1998

Type de dépense	Dépenses de la DGGIST, salaires compris	Dépenses de la DGGIST (sans les salaires)	Dépenses des programmes (sans les salaires)
Dépenses par ETP	2 818 $	1 551 $	3 840 $
Salaires	45 %[1]	0 %	0 %[2]
Matériels	28 %	51 %	38 %
Services de consultation	12 %	22 %	42 %
Communications de données	11 %	20 %	15 %
Logiciels	4 %	7 %	5 %
Fournitures	<1 %	<1 %	<1 %

Ce tableau, qui est basé sur les groupements d'articles d'exécution, montre que le montant dépensé par les programmes (3 840 $) est semblable à celui des dépenses de la DGGIST (2 818 $), bien que les produits et les services soient très différents. Même si la DGGIST engage des consultants pour des fonctions comme le Bureau d'assistance, sa plus grande dépense est au titre des salaires, suivis par les matériels, les consultants et les communications de données, respectivement. Cela présente un contraste marqué avec le profil des programmes. Là, où bon nombre des grands logiciels personnalisés sont mis en œuvre, 42 % des dépenses sont reliées aux services de consultation. Le montant des salaires de la DGGIST confirme qu'il existe une expertise considérable au sein du Ministère. Il est possible qu'une utilisation plus efficace de cette expérience permette de réduire les dépenses des programmes au titre des services de consultation. Il importe également de noter que les dépenses de communications de données sont similaires dans les programmes (15 %) et la DGGIST (20 %). Bien que certaines communications de données soient facturées à l'interne, cela donne à penser que les programmes exploitent des systèmes de communications de données entièrement internes aux secteurs de programmes. Étant donné les contraintes budgétaires actuelles, il semble qu'il serait possible de réaliser des économies si certains de ces systèmes de communications de données étaient regroupés. Selon les discussions informelles que nous avons eues avec des représentants des Services gouvernementaux de télécommunications et d'informatique (SGTI) de Travaux publics et Services gouvernementaux Canada (TPSGC), qui fournissent les services de réseau étendu à la Direction générale des services intégrés et des circuits numériques à la Garde côtière canadienne, il semble que même l'harmonisation de l'acquisition des services permettrait de réaliser des économies et que l'intégration plus étroite de la gestion de ces deux systèmes se traduirait par des économies encore plus importantes. Les liaisons interurbaines de la Garde côtière, qui sont utilisées pour l'information sur la navigation (et pour les communications vocales numérisées), doivent être extrêmement fiables, mais comme les SGTI

[1] Dans ce rapport, les dépenses de la DGGIST au titre des bibliothèques et des dossiers centraux ont été exclues quand l'information sur les dépenses permettait de faire la distinction. Les données proviennent du Système de rapports de gestion financière du MPO, d'Abacus et du Système de gestion des salaires.

[2] Cette étude n'a pas attribué de montants de salaires de programmes aux activités de TI. L'analyse porte plutôt sur les dépenses par article d'exécution, qui est l'information la plus aisément vérifiable. Un examen plus étendu, comme la révision des services votés, serait nécessaire pour déterminer les dépenses salariales directement attribuables à la gestion des TI.

sont les fournisseurs communs, l'harmonisation de la gestion de ces systèmes semblables à l'intérieur du MPO devrait être évaluée.

Tableau 3.2.1.4 Analyse des dépenses de TI par ETP par les programmes et par la DGGIST par région en 1997-1998

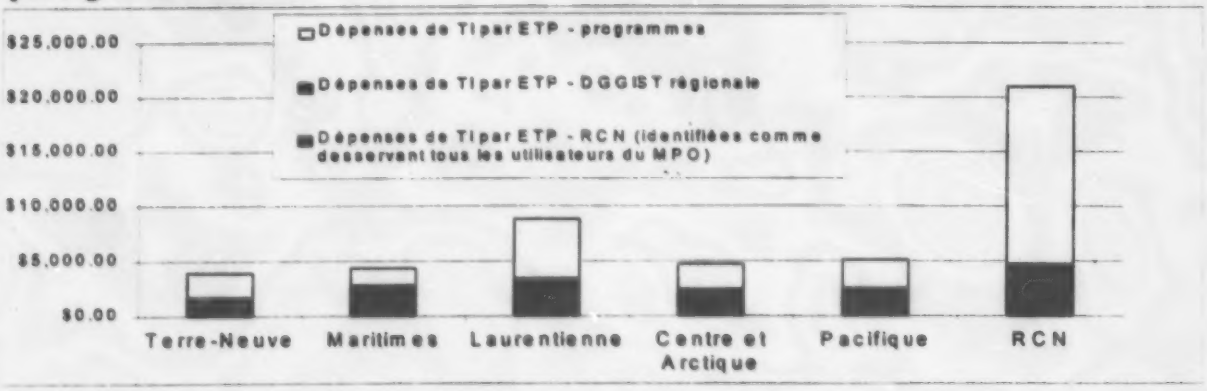


Tableau 3.2.1.5 Dépenses de TI par ETP par région en 1997-1998

Région	Dépenses de la DGGIST dans la RCN identifiées comme desservant tous les utilisateurs du MPO	Dépenses de la DGGIST dans les régions	Dépenses de TI des programmes	Dépenses de la DGGIST dans les régions, en tant que pourcentage de toutes les dépenses de TI des programmes dans cette région
Terre-Neuve	748 $	938 $	2 200 $	43 %
Maritimes	748 $	1 976 $	1 611 $	123 %[3]
Laurentienne	748 $	2 649 $[4]	5 419 $[5]	49 %
Centre et Arctique	748 $	1 638 $	2 352 $	70 %
Pacifique	748 $	1 740 $	2 558 $	68 %
RCN[6]	748 $	4 017 $	16 210 $	25 %
Coût moyen par ETP dans l'ensemble du MPO en 1997-1998 : 6 658 $				

[3] Dans le cadre des accords sur les niveaux de service, plus de 5 millions $ sont transférés des programmes pour les dépenses par la DGGIST.

[4] La région Laurentienne a commencé à faire des dépenses importantes reliées à l'an 2000 en 1997-1998, ce qui pourrait expliquer ce montant plus élevé.

[5] Cette dépense importante comprend deux éléments spécifiques. La région Laurentienne a entrepris d'importants projets An 2000 en 1997-1998. En outre, le système INNAV de la Garde côtière, un système personnalisé de plusieurs millions de dollars destiné à la région Atlantique qui est développé dans la région Laurentienne, est un élément important et exceptionnel qui fait monter les dépenses des programmes par ETP.

[6] Dans cette analyse, la RCN est traitée comme une région, et la DGGIST de la RCN a fait état d'un niveau de dépenses qu'elle identifie comme profitant à tous les utilisateurs du MPO.

Le tableau précédent montre que les modèles de prestation varient considérablement d'une région à une autre. Même les dépenses directes (y compris les salaires) de la DGGIST dans chaque région varient de 25 % des dépenses de TI par les programmes dans la RCN à 123 % des dépenses par les programmes dans les Maritimes. La situation des Maritimes reflète l'important transfert de fonds de programmes à la DGGIST pour les dépenses visées par les accords sur les niveaux de service. Les dépenses de TI sont les plus élevées dans la RCN (quatre fois plus élevées que celles de Terre-Neuve), mais bon nombre des systèmes de programmes nationaux y sont développés et exploités. Ces systèmes (par exemple, le Departmental Violations System, le Habitat Referrals Tracking System et d'autres) entraînent une charge de travail qui est unique à la RCN, à l'exception du système INNAV de la Garde côtière, qui est en voie de développement dans la région Laurentienne en vue d'une application sur la côte Est. Quand les coûts de la DGGIST sont présentés comme un pourcentage de ces systèmes nationaux, la RCN (même avec les dépenses totales de TI les plus élevées par ETP) constitue l'élément le plus petit.

Étant donné la nature essentielle de la fonction de réseautage, il est approprié de fournir un niveau de financement adéquat aux éléments de réseau dans toutes les régions ainsi qu'au réseau étendu (qui est administré dans la RCN pour l'ensemble du Ministère). Une façon d'acheminer les fonds nécessaires pourrait être de fournir les fonds directement de la base ministérielle au début du processus de budgétisation. Il importe de noter que la portion des dépenses ministérielles de TI attribuée au réseau étendu géré par la DGGIST est très petite (à peine plus de 10 % de toutes les dépenses de TI du MPO), comparée à d'autres coûts, malgré le soutien essentiel que ce réseau fournit aux activités ministérielles.

Dans les régions où la DGGIST utilise la facturation interne, des efforts considérables sont déployés pour identifier ce qui est facturé pour le réseau et les éléments connexes. Des efforts mesurables sont également consacrés au recouvrement des créances quand les programmes négligent de verser les sommes convenues, surtout quand certains services (comme le réseau étendu) ne peuvent évidemment pas être retirés pour obliger les débiteurs à payer. Des approches plus cohérentes (par ETP) semblent possibles étant donné l'importante variation montrée ci-dessus.

Tableau 3.2.1.6 Dépenses de TI par ETP sectoriel et par secteur en 1997-1998

Secteur (toutes les régions)	Dépense par ETP sectoriel
Services intégrés	27 385 $[7]
Politiques	5 605 $[8]
Sciences (y compris le secteur Océans)	3 680 $
Garde côtière	3 513 $
Gestion des pêches	2 903 $
Coût moyen par ETP dans l'ensemble du MPO en 1997-1998 : 6 658 $	

[7] Cela comprend non seulement le soutien fourni par la DGGIST au Ministère, mais aussi le soutien d'Abacus, de Peoplesoft et d'autres systèmes, soit un soutien pour tous les secteurs de programmes.

[8] Les deux principaux éléments de cette somme sont les consultants dans les Maritimes (320 000 $) et les matériels dans la RCN (160 000 $)

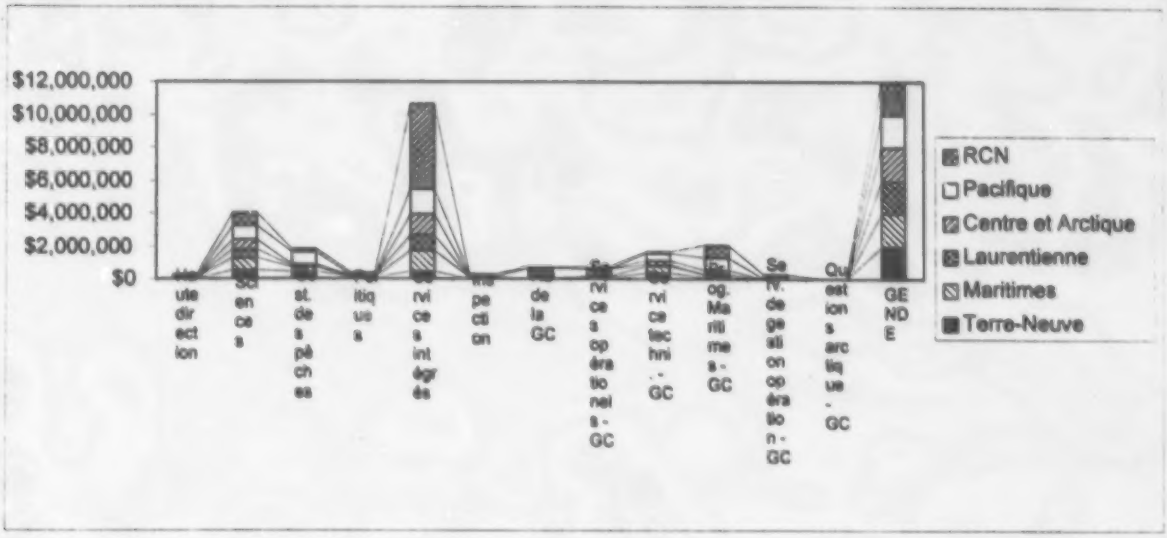
L'analyse précédente montre qu'à l'exception du secteur des Services intégrés, qui héberge non seulement la fonction DGGIST mais aussi Abacus et Peoplesoft, les dépenses TI des programmes par ETP sont sur la même échelle. Il vaut la peine de le mentionner car le secteur des Sciences est souvent considéré comme un très important utilisateur de TI; cependant, sur la base des dépenses par ETP, il est au même niveau que la Garde côtière et sur un niveau semblable à celui de la Gestion des pêches. Il importe de souligner que, compte tenu du rôle de soutien des Services intégrés au sein du Ministère, les dépenses « par ETP des Services intégrés » ne peuvent pas être facilement comparées aux dépenses des autres secteurs, mais ont été incluses pour des raisons d'exhaustivité.

Plusieurs investissements « ponctuels » dans les TI ont été effectués au cours des trois derniers exercices. Chacun de ces investissements a procuré des avantages mesurables et conformes aux objectifs d'investissement. Ce qui n'a pas été prévu, c'est la fourniture de fonds stables, sur une base continue et à long terme, pour assurer le fonctionnement des activités de base et leur évolution en fonction des besoins. Ces investissements « ponctuels » (comme le Projet de courrier électronique et d'infrastructure communs) peuvent solutionner des problèmes de « rattrapage » spécifiques; cependant, il serait possible d'éviter ce genre de dépenses urgentes de rattrapage/dérouillage en reconnaissant le besoin d'assurer la maintenance continue des fonctionnalités de base. Ces fonctionnalités de base peuvent être définies au moyen des consultations clients-fournisseurs sectorielles recommandées ailleurs dans ce rapport, mais comprendraient probablement le réseau étendu et les RL, les systèmes d'exploitation, la suite de bureautique, le Bureau d'assistance et la désignation de gestionnaires de portefeuilles de TI, et les l'évolution nécessaire de ces systèmes en fonction des besoins.

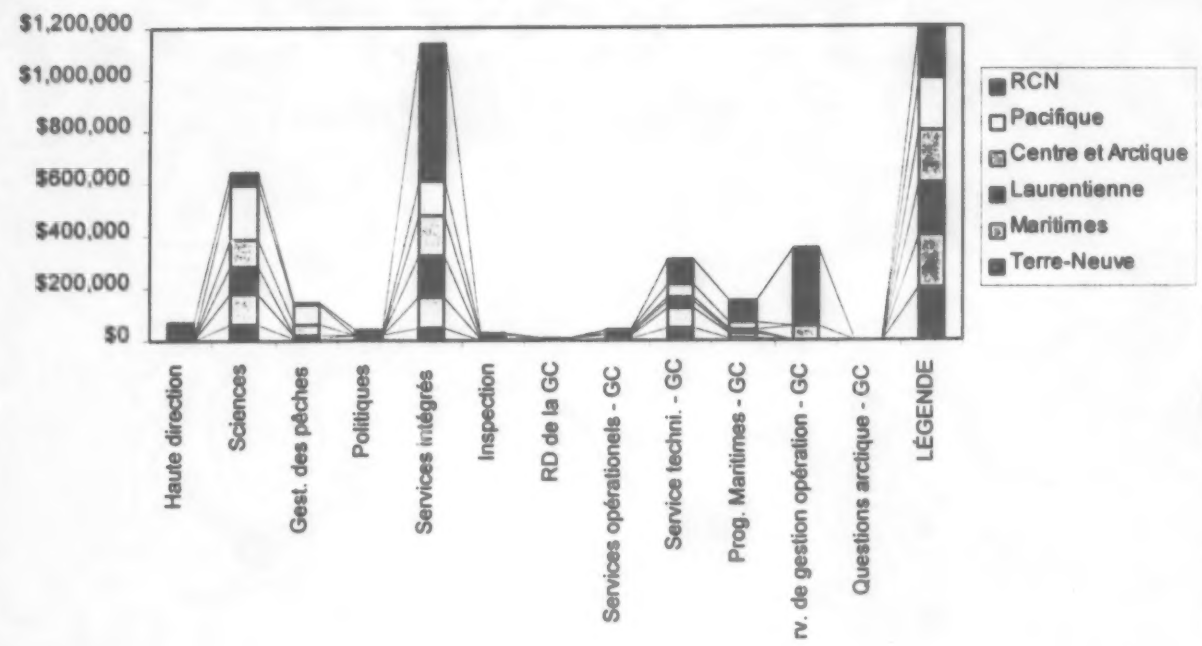
Les dépenses du Ministère se répartissent en quatre grands groupes d'articles d'exécution. Une comparaison des schémas de dépenses du MPO et d'autres ministères ayant des missions semblables est présentée ci-après. Les schémas de dépenses, quand ils sont présentés par groupes d'articles d'exécution, par secteur (et par branche d'activité pour la Garde côtière) et par région, aident à identifier comment les stratégies de gestion des TI diffèrent. L'information est présentée par groupes d'articles d'exécution, comme suit : matériels, logiciels, services de consultation et communications de données. Les catégories secteur et branche d'activité correspondent aux barres individuelles, et la région à l'origine des dépenses est représentée par un schéma de marquage systématique. Quand les graphiques changent d'échelle, la valeur de la barre la plus élevée est indiquée dans chaque graphique.

Tableau 3.2.1.7 Dépenses de TI par groupe d'articles d'exécution, par région et par secteur ou branche d'activité, en 1997-1998

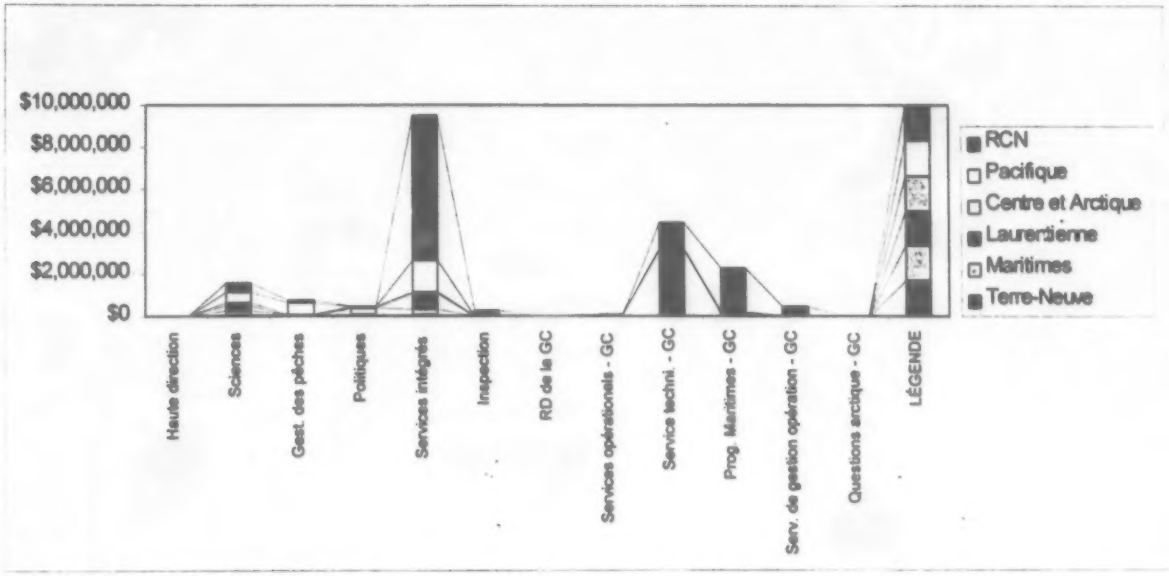
Dépenses de matériel – 1997-98
Total de 22,7 millions $



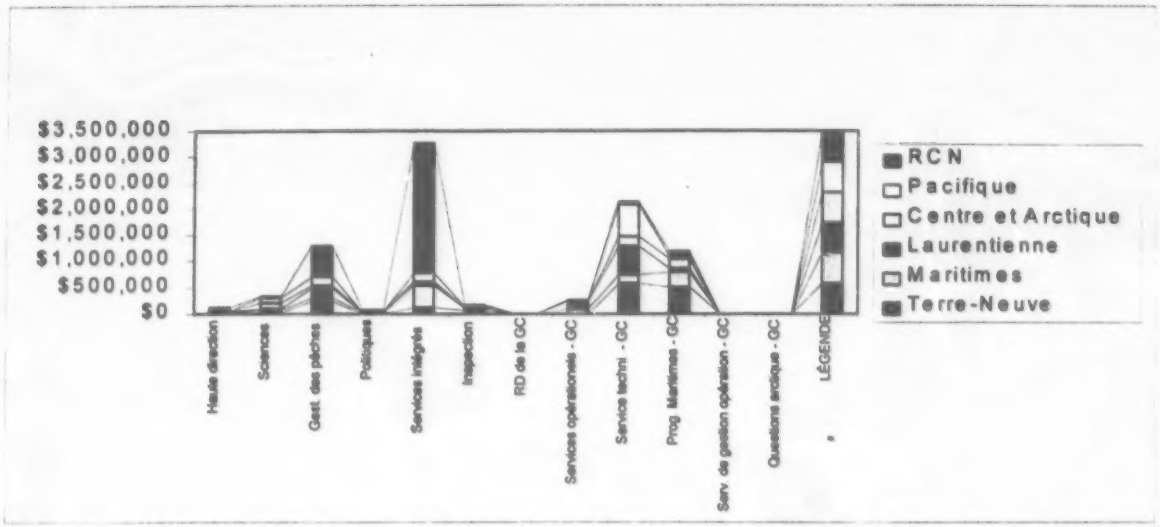
Dépenses de logiciels – 1997-98
Total de 2,9 millions $



Dépenses de consultations – 1997-98
Total de 2,9 millions $



Dépenses de télécommunications 1997-98
Total de 8,9 millions $



3.2.2 Comparaison des dépenses avec celles d'autres ministères et organismes

Nous avons analysé les données sur les dépenses (par article d'exécution) de tous les ministères et organismes fédéraux. Tous les ministères sont différents, mais nous avons choisi les dépenses des trois autres ministères de « ressources naturelles » (Environnement Canada, Ressources naturelles Canada et Agriculture et Agro-alimentaire Canada) et celles de Santé Canada, car elles sont suffisamment semblables pour permettre de faire des comparaisons.

Nous avons évalué toutes les dépenses ministérielles en tant que coûts par ETP et que pourcentage du budget global (moins les subventions et les contributions). Tel qu'indiqué, dans cet exemple, les coûts du MPO sont tirés des mêmes tableaux que ceux des autres ministères et ne comprennent donc pas les dépenses (comme les salaires de la DGGIST) qui sont étudiées dans les autres parties de l'examen.

Tableau 3.2.2.1 Dépenses de TI des ministères à mission semblable en 1997-1998

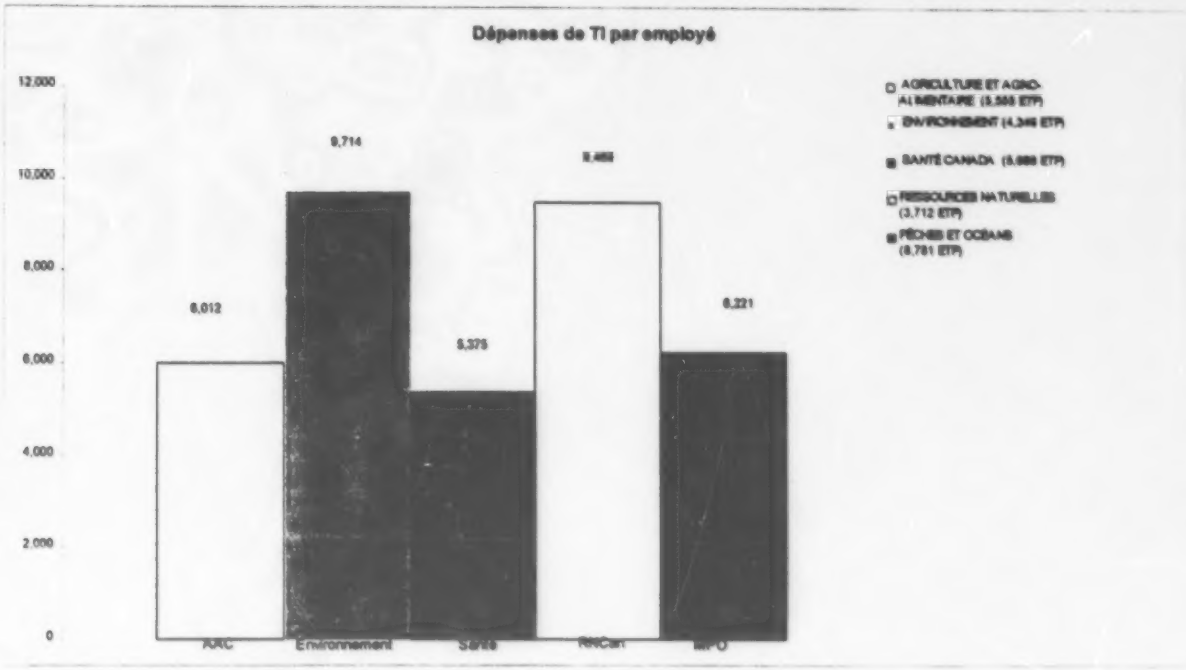
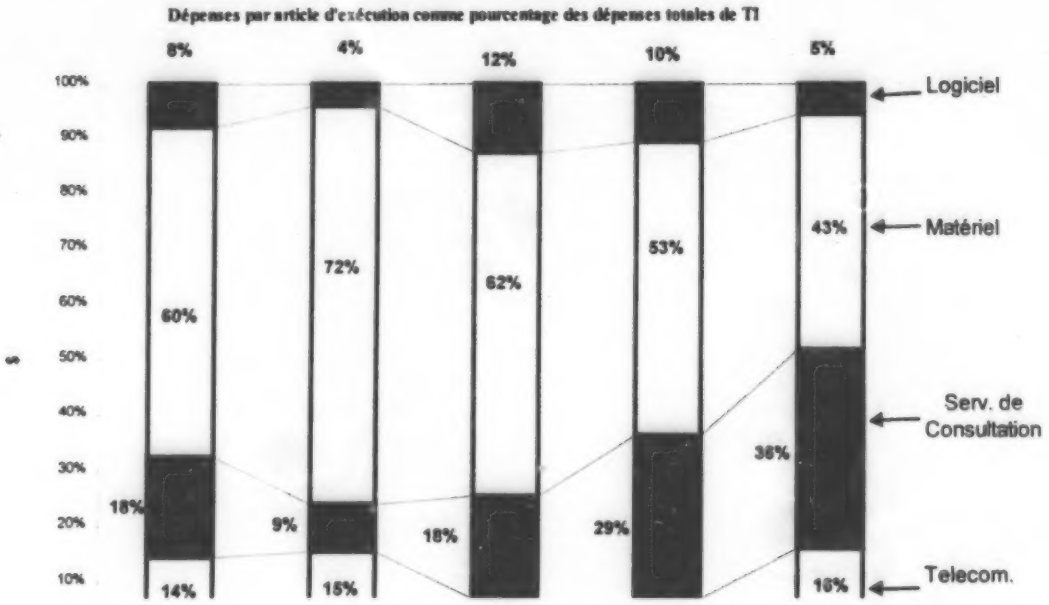


Tableau 3.2.2.2 Dépenses de TI des ministères semblables, en tant que pourcentage du budget de base, en 1997-1998

Ministère	Dépenses par ETP	Pourcentage du budget de base
Santé Canada	5 375 $	2 %
Agriculture et Agro-alimentaire Canada	6 012 $	2 %
MPO (données du SCT)[9]	6 221 $[9]	4,8 %[9]
Ressources naturelles Canada	9 469 $	7 %
Environnement Canada	9 714 $	7,6 %

[9] Les données du Secrétariat du Conseil du Trésor ne comprennent pas les salaires ni pour le MPO, ni pour les autres ministères, ce qui explique la différence entre le montant indiqué ici pour le MPO et les dépenses totales de 6 658 $ par ETP pour le MPO utilisées partout ailleurs dans ce rapport.

Tableau 3.2.2.3 Dépenses de TI des ministères semblables, par groupe d'articles d'exécution en 1997-1998



Cette analyse des dépenses, qui montre le pourcentage des dépenses totales de TI par groupe d'articles d'exécution, révèle qu'il y a d'importantes variations entre les cinq ministères dans la manière dont les budgets de TI sont dépensés. Le MPO a les dépenses de matériels les moins élevées, mais il dépense plus, en pourcentage, pour les services de consultation que n'importe lequel de ces autres ministères.

Le tableau suivant montre les dépenses « par ETP » des entreprises nord-américaines, ainsi que celles des gouvernements américains aux paliers fédéral, étatique et local. Nous avons inclus ce tableau car, durant la discussion du rapport intérimaire au Comité d'examen ministériel, on nous a demandé de situer les dépenses du MPO dans un contexte plus large comprenant le secteur privé. Il vaut la peine de mentionner que, malgré les nombreuses faiblesses de ce type de comparaison globale, les dépenses du MPO par employé sont sur la même échelle que celles des entreprises d'Amérique du Nord. Ce tableau montre aussi que les dépenses de TI sont fortement asymétriques et que si 50 % des entreprises dépensent moins de 7 000 $ par employé, ces dépenses grimpent à plus de 24 000 $ lorsqu'on ajoute 75 % des entreprises. Cela reflète probablement le niveau d'utilisation des TI à des fins d'affaires. Cette information sert surtout à indiquer que, dans le cas des entreprises qui dépendent fortement des technologies, les coûts par ETP peuvent atteindre des niveaux très élevés. Cela est particulièrement apparent au gouvernement fédéral américain, où 50 % des organisations dépensent moins de 1 500 $, tandis que 75 % d'entre elles dépensent plus de 25 000 $, encore plus que les entreprises comparables. Ces comparaisons globales sont moins pertinentes pour le MPO que l'évaluation précédente des ministères canadiens semblables, si ce

F2

n'est l'observation que les dépenses de TI peuvent présenter une différence considérable (de l'ordre de 16 fois plus) entre les organisations peu dépendantes des solutions de TI et celles qui les mettent en œuvre de façon plus généralisée.

Tableau 3.2.2.4 Dépenses de TI (en $ Can) au gouvernement et dans l'industrie, en 1997-1998

Organisation	**25 % dépensent moins que cela par employé**	**50 % dépensent moins que cela par employé**	**75 % dépensent moins que cela par employé**	**50 % affectent aux TI ce pourcentage des dépenses totales**
Entreprises nord-américaines	2 208 $	6 996 $	24 012 $	2,9 %
Gouvernements américains - États et municipalités	3 585 $	11 481 $	35 881 $	0,8 %
Départements du gouvernement fédéral américain	810 $	1 472 $	25 636 $	1,7 %
Les dépenses réelles du MPO sont de 6 658 $ par employé, soit 6,5 % des dépenses totales.				

L'analyse des ministères fédéraux canadiens indique que les TI constituent une portion importante des dépenses ministérielles et que les dépenses de TI du MPO sont généralement sur la même échelle que celles des autres ministères de ressources naturelles. Il est difficile de faire des projections futures de ces dépenses, car il y a une différence concrète de coûts entre un modèle statique basé sur les besoins et une approche basée sur la mise en œuvre énergique des TI dans de nouveaux domaines. Ce rapport examine, entre autres choses, comment ces dépenses sont faites dans les différents secteurs du Ministère et dans quelle mesure des changements pourraient améliorer la performance et la valeur.
La façon la plus efficace d'éliminer les chevauchements et les inefficiences est de consulter, de coopérer et de regrouper, dans le but d'atteindre la cohérence et l'uniformité. Il existe des organisations et des approches qui peuvent réduire considérablement les coûts (par exemple, un contrôle très centralisé, une liste restreinte de matériels et de logiciels approuvés), mais il n'est pas certain que les besoins des programmes et les traditions de gestion du MPO permettraient de les appliquer. La stratégie qui présente le plus grand potentiel de succès repose sur une véritable coopération entre clients et fournisseurs, ainsi que sur l'appréciation des avantages du regroupement. Nous avons constaté que ce modèle existe, habituellement pour des initiatives ou des projets précis, dans les Maritimes, dans la région Laurentienne, dans la région du Pacifique et dans la RCN.

Le Ministère réalisera des avantages tangibles en traitant le réseau (comprenant le courriel, la suite de bureautique et l'assistance utilisateur) comme un actif ministériel. Pour ce faire, ce groupe de spécialistes (la DGGIST) doit recevoir des fonds suffisants non seulement pour fonctionner, mais aussi pour poursuivre cette activité et la faire évoluer. Dans plusieurs régions, des « gestionnaires

de portefeuilles » sont désignés par la DGGIST pour devenir des experts des besoins d'un secteur d'activité particulier. Dans les régions où ces postes existent et où il y a de bons liens avec les secteurs de programmes, nous avons constaté qu'il s'agissait d'une « pratique optimale » qui contribuait pour beaucoup à instaurer la coopération et la cohérence.

Une recommandation clé de ce rapport a également été formulée dans le rapport sur la DGGIST réalisé en 1994 par Price Waterhouse, à savoir : « mettre fin à la pratique de la facturation interne pour les services de gestion des RL. Ces services devraient être financés au niveau ministériel. » Cette recommandation vaut toujours et sa mise en œuvre contribuerait pour beaucoup à résoudre les problèmes d'incohérence et de niveaux inadéquats de services dans certaines régions, de même qu'à réduire le temps et les efforts consacrés à la perception des comptes internes. Pour y arriver, il faut définir clairement ce qui est compris et ce qui ne l'est pas, et évaluer de façon explicite et vérifiable le niveau de financement qui devrait être fourni (peut-être par l'intermédiaire de la structure de comités proposée dans la section « Recommandations » de ce rapport).

Il n'est pas possible d'établir clairement le niveau de financement sans décider si la stratégie poursuivie consistera à soutenir adéquatement les objectifs des programmes ou si elle visera à permettre au MPO d'être à la fine pointe, ou presque, de la mise en œuvre des TI. Les niveaux de risques et de dépenses varient considérablement entre un Ministère qui est un gestionnaire efficient des TI et un Ministère qui est « à la fine pointe » de la technologie.

3.3 RÉGIE

3.3.1 Rôles et responsabilités

Une constatation générale importante, que nous avons pu faire dans toutes les filières d'enquête, était l'absence d'application de politiques pertinentes et significatives. Dans certains cas, il s'agit d'une absence complète de toute politique, tandis que dans d'autres cas, c'est l'application des politiques existantes qui fait défaut. Les politiques les plus importantes ici sont du type « qui fait quoi? » et « comment procéder ».

L'absence de politiques (ou l'inapplication de celles qui existent) s'est traduite par un ensemble d'approches disparates. Cette faiblesse a des incidences particulièrement graves sur les activités du MPO dans le domaine des grands systèmes personnalisés. La deuxième faiblesse en importance concerne l'acquisition de matériels et de logiciels. Un autre domaine où l'on constate un manque de cohérence correspond aux services dont la DGGIST est responsable dans différentes régions. Il y a aussi un manque de cohérence en ce qui concerne la présence ou l'absence ainsi que le niveau de facturation interne aux programmes. Certaines régions (comme la région du Pacifique) conservent d'importants niveaux d'expertise en TI dans les secteurs de programmes, tandis que d'autres (comme les Maritimes) ont délibérément transféré du personnel des programmes à la DGGIST. On trouve même une situation médiane (comme la région Laurentienne), où le personnel des programmes est « dirigé fonctionnellement » par les Services intégrés tout en demeurant dans les secteurs de programmes. Ce rapport identifie un nombre important de domaines qui pourront gagner en cohérence si l'on accroît la coopération et la consultation entre le personnel des programmes et le personnel de la DGGIST. Pour procurer tous

les avantages possibles, cette coopération doit s'accompagner d'ententes claires quant aux points sur lesquels les comités régionaux pourront faire des recommandations exécutoires en matière de dépenses et ceux pour lesquels leur rôle sera uniquement consultatif.

3.3.2 Le besoin d'approches consultatives entre clients et fournisseurs

Dans les rapports préparés en 1993 et en 1994 par Price Waterhouse, l'on recommandait l'établissement de comités clients-fournisseurs qui faciliteraient l'utilisation des TI. Ce besoin demeure aujourd'hui. Dans toute relation de service réussie, les besoins du client doivent guider la prestation des services. Il y a deux paliers : les services qui sont fournis sans frais et les services à facturation interne. En ce qui concerne le premier palier, il est important de se doter d'un mécanisme qui fasse en sorte que les demandes correspondent réellement aux besoins. Ce mécanisme pourrait être l'approbation obligatoire, par tous les secteurs, de l'évolution des services à financement de base, étant donné que les secteurs pourraient être obligés d'accepter des niveaux inférieurs de financement général si de nouveaux niveaux de services étaient définis comme étant « de base ».

Il existe actuellement des mécanismes consultatifs clients-fournisseurs dans divers secteurs et régions, mais pas de schéma définissable. Au niveau régional, nous avons trouvé des comités qui avaient été mis sur pied pour des projets spéciaux précis. Dans quelques rares cas, des comités multisectoriels régionaux avaient été formés et, dans certains cas, les membres estimaient qu'ils fonctionnaient bien. Nous avons également trouvé des comités où un secteur collabore avec la DGGIST pour répondre aux besoins d'un programme précis. Ces comités se retrouvent surtout dans la région du Pacifique, où les ressources de TI peuvent être facilement identifiées comme relevant des programmes.

Au niveau national, il n'existait pas de structure de comités clients-fournisseurs au moment où nous avons réalisé cet examen. Un comité composé des directeurs de la DGGIST invite périodiquement les membres subalternes de la Direction générale, mais ces réunions élargies ne surviennent qu'une ou deux fois par année. Un comité national clients-fournisseurs (appelé le Comité ministériel de travail sur l'informatique) ne s'est pas réuni depuis plus d'un an et semble avoir été dissout. Au début de 1999, le SMA des Services intégrés a créé le Comité directeur de l'informatique (CDI) qui représente tous les secteurs du MPO et fournira des orientations en matière de TI. Il s'agit là d'une bonne mesure de base qui permettra de résoudre plusieurs questions importantes identifiées dans cet examen.

Il est clairement nécessaire d'avoir au moins deux niveaux de discussions clients-fournisseurs. Le premier serait un forum de niveau supérieur ayant certaines des responsabilités qui ont été proposées pour le nouveau CDI. Pour être efficace, ce comité de haut niveau doit être appuyé par d'autres structures mieux à même de résoudre des questions détaillées et spécifiques aux secteurs ou aux régions. Ces autres structures/comités pourraient examiner comment le Ministère devrait traiter les nouvelles utilisations des TI qui imposent au réseau étendu/RL de nouvelles demandes plus importantes que le simple courriel ou le partage de textes. Il y a actuellement plusieurs cas (dont le système INNAV et les multimédias) qui, s'ils étaient mis en œuvre, exerceraient des pressions excessives sur la capacité actuelle du réseau. Les comités et les groupes de travail qui

appuient le CDI pourraient se concentrer sur les utilisations stratégiques à long terme des TI. Ces utilisations sont quasi illimitées, et il faut apparier les besoins et les souhaits des programmes avec les facteurs coûts, la faisabilité technique et l'opportunité. Étant donné les coûts et la complexité associés à l'utilisation à grande échelle des solutions de TI (comme le montrent, dans la section précédente, les données sur les dépenses qui indiquent une augmentation rapide des dépenses entre les organisations moyennes et au-dessus de la moyenne), il importe que les « projets pilotes » soient bien conçus et que les résultats soient largement communiqués. Cela se fait actuellement à très petite échelle dans quelques secteurs, mais il n'y a aucun partage généralisé des expériences et des idées.

Le MPO pourrait aussi profiter grandement d'une mise à jour utilisateur-fournisseur de la norme d'architecture informatique. La création du document sur l'architecture informatique du MPO et les initiatives d'infrastructure subséquentes qui ont été réalisées dans la foulée de ce document ont grandement amélioré l'interopérabilité technique du réseau et de ses systèmes. Certains problèmes touchant la planification, le financement et la gestion des actifs informatiques dans l'ensemble du Ministère doivent cependant être résolus pour que ces réseaux fonctionnent réellement et répondent efficacement aux besoins du Ministère.

L'Examen de la restructuration des Services intégrés qui s'est récemment terminé indiquait que, dans le secteur de la DGGIST, les clients insistaient sur le besoin de consulter les gestionnaires de services. L'analyse réalisée à l'appui de l'Examen de la gestion des technologies de l'information indique qu'il est également très nécessaire que les gestionnaires de programmes consultent le personnel de la DGGIST dans un large éventail de domaines, dont le plus important est celui des grands systèmes informatiques et des applications logicielles personnalisées. Il est également clair, cependant, que même les questions quotidiennes pourraient être mieux coordonnées et résolues de façon plus efficace si la gestion des technologies de l'information était basée sur des approches intégrées. Pour réussir, les grandes initiatives complexes devraient être planifiées et réalisées avec la participation de la DGGIST, et de façon compatible avec les approches ministérielles.

3.3.3 Les grands systèmes

Nous avons étudié les grands systèmes du MPO afin d'évaluer les structures de gestion implicites et explicites en rapport avec ces systèmes qui entraînent d'importantes dépenses de TI. Ce volet de l'examen visait les grands systèmes de la RCN et dans une région (les Maritimes). Notre intention était d'évaluer la gestion de ces systèmes de leur conception à leur mise en application ou à leur mise en œuvre complète (lorsque cela était possible). Les grands systèmes sont définis comme des systèmes personnalisés coûtant plus de 500 000 $, fournis à plus de 100 employés ou mis en œuvre dans de multiples sites.

Il n'existe pas d'approche unique au MPO pour le développement et la mise en œuvre des grands systèmes. Dans les secteurs public et privé, il existe plusieurs modèles de planification et de développement qui se sont révélés efficaces pour contrôler les coûts et produire les résultats attendus. Au moins deux des systèmes du MPO que nous avons examinés sont passés d'un coût prévu de moins de 100 000 $ à un coût de livraison de plus de 1 million $ (le Departmental Violations Information System et le Habitat Referrals Tracking System). Dans l'ensemble, nous

avons constaté que les systèmes qui avaient été développés par des équipes de projet spécifiques, comprenant du personnel de la DGGIST, des utilisateurs et des consultants (s'il y avait lieu), étaient ceux qui fonctionnaient le mieux. En d'autres termes, ces systèmes ont été développés en harmonie avec l'architecture technique et en tenant compte des besoins des utilisateurs, auxquels ils répondent. Dans les cas où il n'y avait pas de plans détaillés comprenant des jalons précis et des descriptions claires de ce que le système était censé faire, les coûts étaient plus élevés que prévu et, dans certains cas, les produits livrables n'avaient pas été fournis pendant l'exercice au cours duquel ils étaient attendus.

Il faut prévoir dès le départ le soutien de l'infrastructure de ces grands systèmes, ainsi que l'évolution et la maintenance des systèmes eux-mêmes et la formation des utilisateurs. Dans certains cas, le soutien des systèmes a été facturé aux programmes par la DGGIST. Quand les coûts et les niveaux de soutien n'avaient pas été établis au début du processus, les discussions qui ont eu lieu par la suite ont été décrites comme étant difficiles.

Lorsque les programmes développent de très grands systèmes, ils risquent aussi de mettre en œuvre des réseaux parallèles au système existant. Les circuits numériques interurbains de la Garde côtière et les propositions associées au projet INNAV sont très similaires, du point de vue des matériels et de l'architecture, au réseau étendu exploité par la DGGIST. Les SGTI sont les fournisseurs des liaisons interurbaines de la Garde côtière et des systèmes de la DGGIST. Lors des rencontres avec l'équipe d'examen, les représentants des SGTI ont indiqué qu'il serait possible de réduire les coûts en regroupant l'acquisition de ces services. À l'évidence, une évaluation des économies potentielles permises par ce regroupement s'impose. En réalité, l'information qui circule dans ces systèmes et la tolérance aux défaillances de l'activité sont différentes, mais les matériels et les liaisons interurbaines sont dans bien des cas similaires, et le fournisseur est le même (les SGTI).

En conclusion, une approche coordonnée au développement et à la mise en œuvre des grands systèmes est une amélioration importante de la régie que le MPO devrait envisager. Ces systèmes sont non seulement coûteux, mais, dans certains cas, des systèmes aux fonctions identiques sont développés indépendamment dans différents secteurs et régions (comme les systèmes de licence et d'information sur la gestion des pêches). Les avantages de l'utilisation d'une approche intégrée centrée sur le client comprennent des économies de coûts ainsi que des solutions plus robustes car les expériences et les approches d'une région ou d'un secteur peuvent être utilisées pour améliorer les résultats d'autres secteurs ou régions.

3.3.4 L'administration du réseau étendu de la DGGIST

Cette partie de l'examen porte sur la gestion des « conduites » d'information qui transportent l'information entre les édifices et les villes. En langage informatique, la taille de ces conduites est appelée « largeur de bande » et leur usage est appelé « charge » ou « utilisation de la largeur de bande ». Comme dans l'exemple des conduites, il est possible de « dimensionner » ces liaisons (plus elles sont grosses, plus elles sont coûteuses) et il est possible de les remplir tellement que tout le système ralentit et finit par tomber en panne.

Les liaisons appartiennent à deux catégories générales. La première est le réseau étendu (RE), qui est géré et financé par la DGGIST de la RCN. La deuxième est constituée des réseaux locaux (RL), qui sont les liaisons gérées par les régions depuis leurs bureaux régionaux. La complexité varie entre les régions du Centre et de l'Arctique, où toutes les liaisons interurbaines sont exploitées comme des éléments du RE, et les régions du Pacifique, des Maritimes et la région Laurentienne, où des liaisons interurbaines et optiques de grande capacité sont gérées par les administrations régionales.

Le RE de la DGGIST, qui relie 94 ordinateurs du MPO (c.-à-d. des routeurs) dans tout le Canada, est le principal système de communication interurbaine pour le courriel, les applications de bureautique et les données. L'administration quotidienne de ce réseau est impartie aux Services gouvernementaux de télécommunications et d'informatique (SGTI) de Travaux publics et Services gouvernementaux Canada (TPSGC). Les SGTI ont confié la gestion du système à une entreprise privée locale appelée NUVO Networks.

L'information sur le processus de gestion qui a abouti à l'attribution de ce contrat aux SGTI indique que les procédures habituelles n'ont pas été suivies. Les gestionnaires de RL régionaux disent avoir été simplement informés que les services seraient fournis par les SGTI, sans consultation des organisations régionales clientes. L'Équipe d'examen a appris que lorsque le contrat du MPO a été attribué aux SGTI, la gestion des 94 routeurs venait doubler la responsabilité des SGTI. La gestion de ce contrat ne semble pas refléter le type de consultation et de coordination qui est souhaitable. En outre, tel qu'indiqué ci-après, les dispositions contractuelles présentent plusieurs faiblesses.

Il existe actuellement un Accord sur les niveaux de service (ANS) détaillé entre le MPO et les SGTI. L'examen de ce document, ainsi qu'une série d'entrevues avec des représentants du MPO et des SGTI, démontrent qu'il y a des faiblesses dans le document actuel, notamment :

1. Les services que les SGTI doivent fournir au MPO ne sont pas définis de façon détaillée, bien qu'il y ait des références directes à la disponibilité du réseau et aux mesures de résolution de problèmes précis.

2. Les SGTI mesurent leur performance en fonction de la disponibilité du réseau, mais ne sont aucunement tenus d'indiquer quand la disponibilité spécifiée n'est pas assurée. En outre, si la disponibilité spécifiée n'est pas assurée, il n'y a pas de pénalités pour les SGTI ou de compensations financières pour le MPO. La disponibilité du réseau semble donc constituer une « cible » plutôt qu'une norme. Un niveau de service qui lierait davantage les SGTI préciserait ce que le MPO achète exactement et quelles conséquences ou actions découlent du défaut de prestation de ce niveau de services.

Selon les dispositions actuelles, le MPO reçoit des rapports quotidiens, hebdomadaires et mensuels des SGTI/NUVO. Ces rapports sont si généraux qu'ils n'ont aucun sens pour le personnel des SGTI et du MPO. La défaillance totale d'une liaison particulière du réseau est signalée à la DGGIST de la RCN si elle ne peut pas être réparée dans les deux heures qui suivent (un jour

ouvrable), mais les pannes totales sont beaucoup plus rares qu'une surcharge du réseau qui ralentit toutes les communications, y compris le courrier électronique et les sessions Abacus.

En outre, les rapports ne sont pas stratifiés de façon à présenter séparément les six liaisons qui sont essentielles aux communications inter-régionales. La liaison du RE à Vancouver, par exemple, supporte toutes les communications réseau à l'intérieur de la région et avec les autres régions. Sa défaillance affecte donc les 2 344 membres du personnel de la région du Pacifique et la capacité du reste du MPO de les joindre. Cette situation est entièrement différente de celle qui pourrait survenir si la liaison à un petit bureau sous-régional tombait en panne et que seuls les quelques employés de ce bureau étaient affectés. Le système de rapports quotidiens actuellement assuré par NUVO traite ces deux liaisons de façon identique.

Nous avons réalisé une analyse détaillée de l'architecture du réseau. À cause de la nature de la gestion des RL et du RE, il a été difficile d'identifier tous les équipements reliés au RE et aux RL. Une fois qu'une « topologie » complète a été préparée, il est devenu clair que le réseau du MPO reflète son histoire, à savoir qu'on l'a assemblé en reliant une variété de sous-éléments, au lieu de le concevoir comme un tout.

Les SGTI, qui sont chargés de formuler des recommandations architecturales dans le cadre du présent accord sur les niveaux de service, ne l'ont pas fait. Le consultant en informatique qui a réalisé ce volet de l'examen a indiqué que le MPO pourrait réaliser des économies de coûts au chapitre de la gestion du réseau et accroître la sécurité et la performance en mettant en œuvre une architecture intégrée à l'échelle du Ministère. Le fait que les SGTI n'aient pas fourni de recommandations architecturales permettant d'améliorer la performance et de réduire les coûts, recommandations qui sont prévues dans le contrat, est considéré par l'équipe d'examen comme une lacune grave. Comme le contrat ne prévoit aucune pénalité, il semble qu'on ne puisse pas faire grand-chose pour remédier à cette situation jusqu'à ce que ces travaux fassent l'objet d'un nouvel appel d'offres au cours du prochain exercice.

La gestion efficace de la « largeur de bande » est l'une des mesures les plus apparentes du service aux clients. Quand les liaisons réseau deviennent surchargées, il y a augmentation du temps que l'information met pour voyager sur le réseau. Cela est particulièrement évident pour les utilisateurs quand des applications essentielles comme Abacus, Peoplesoft et, dans certaines régions, Word et Excel sont livrées à partir d'un site central. Si le courrier électronique prend quelques minutes ou quelques secondes, cela est rarement apparent pour les utilisateurs; cependant, si un utilisateur entre des données ou prépare un rapport, et qu'il doit attendre plusieurs minutes pour que l'application réagisse, cela est très frustrant et peut entraîner des problèmes reliés à l'application. Ainsi, une fonction de gestion du réseau consiste à surveiller le niveau de « trafic » sur les liaisons réseau et à s'assurer que le niveau de service est bon dans les circonstances « normales ».

Les rapports que les SGTI fournissent actuellement au MPO ne tiennent compte que des dix liaisons les plus occupées. Dans plusieurs cas de surcharge des liaisons, il n'existe aucun remède, car la compagnie de téléphone locale offre un service limité dans la région. Dans d'autres cas de ralentissement des grandes liaisons inter-régionales, il n'existe pas d'étapes établies et explicites à

suivre. La gestion actuelle du RE utilise trois approches. L'évaluation de plusieurs exemples n'a pas permis de déterminer comment une approche est choisie de préférence à une autre. L'équipe d'examen a demandé qu'on lui fournisse les lignes directrices écrites qui s'appliquent à ces décisions de gestion et a appris qu'il n'en existait pas.

Quand les liaisons deviennent si occupées que la performance se dégrade, les options sont : ne rien faire, augmenter la capacité de la liaison ou interdire l'utilisation de certaines applications. La première approche était apparente dans les discussions avec les membres de la DGGIST, qui ont indiqué que, dans le cas de certains petits bureaux du MPO qui auraient besoin d'une augmentation de la capacité, il n'y a pas de fonds disponibles pour acheter les équipements et les services nécessaires. À titre d'exemple de la deuxième stratégie, la capacité de six liaisons RE a été augmentée en octobre 1998, ce qui démontre qu'en certaines circonstances, il y a acquisition de capacité accrue. Un exemple de la dernière stratégie réside dans les mesures prises pour la liaison RE reliant la région de Terre-Neuve au reste du MPO. Dans ce cas, les utilisateurs d'Abacus à Terre-Neuve trouvaient que le RE était très lent. Au lieu de ne rien faire ou de faire l'acquisition d'une capacité accrue, on a décidé de retirer l'accès multimédia à tous les utilisateurs de Terre-Neuve, de la RCN et de la région du Centre et de l'Arctique. Les utilisateurs du réseau n'ont pas été consultés ni avisés de ce changement. De plus, quand des ajustements seront faits pour rediriger le trafic Internet de Terre-Neuve vers un système coupe-feu régional, il n'est pas clair si l'accès multimédia sera rétabli pour les utilisateurs de la RCN et de la région du Centre et de l'Arctique.

Les SGTI ont la responsabilité d'identifier les liaisons réseau surchargées, de communiquer les solutions au MPO et d'appliquer ces solutions. Même si l'accord sur les niveaux de service stipule que ce type d'analyse fait partie des attributions des SGTI, le personnel du MPO réalise régulièrement ces analyses, et toutes les récentes mises à niveau des liaisons ont été faites par suite du travail du personnel du MPO, et non de celui des SGTI.

3.3.5 Le besoin de soutien des TI en dehors des heures normales de travail

Les programmes du MPO, en particulier ceux qui se rapportent aux interventions d'urgence, doivent toujours fonctionner efficacement. De nombreuses activités essentielles dépendent du RE et des RL, et les approches traditionnelles du télécopieur et du téléphone servent d'appoint à ces approches réseau. Comme les technologies jouent un rôle de plus en plus essentiel, cette capacité d'utiliser les « anciennes méthodes » diminuera en efficacité, augmentant de ce fait le besoin de réduire les points de défaillance du RE et des RL. Durant cet examen, les gestionnaires de programmes se sont souvent montrés inquiets du fait qu'en raison de la dépendance accrue des programmes envers l'infrastructure de TI, le réseau étendu et les RL doivent assurer une performance totalement fiable, 24 heures par jour, 7 jours par semaine.

À l'heure actuelle, seulement 6 des 94 routeurs du MPO sont supportés 24 heures sur 24. Tous les autres routeurs du réseau étendu et des RL ne sont supportés que durant les heures normales de travail. Les liaisons interurbaines de la Garde côtière sont supportées 24 heures par jour quand la mission du programme l'exige. Pour regrouper les fonctions de TI qui relèvent actuellement de la

Garde côtière et de la DGGIST, il faut s'assurer que les besoins des clients seront entièrement satisfaits en dehors des heures normales de travail.

Les évaluations de la menace et des risques recommandées dans la section de ce rapport portant sur la sécurité peuvent servir à identifier les autres éléments existants du RE et des RL qui doivent être supportés 24 heures par jour. Il semble que le courrier électronique, qui est très utilisé, spécialement durant les interventions d'urgence lors de déversements et d'accidents en mer et durant les activités relatives à l'application des lois sur les pêches, devrait être supporté 24 heures sur 24. Il faut souligner que, en raison des coûts engagés pour payer le personnel en disponibilité et la facturation interne, il serait coûteux d'assurer un soutien permanent dans toutes les régions.

3.4 LE BESOIN DE POLITIQUES

3.4.1 Aspects généraux nécessitant des améliorations

Une importante constatation générale, qui touche tous les volets de l'enquête, était la nécessité de mettre en œuvre des politiques du genre « qui fait quoi » et « comment ». Dans certains cas, le problème est l'absence d'une politique applicable, dans d'autres cas, c'est l'inapplication de la politique existante.

Les aspects généraux nécessitant des orientations politiques pertinentes et significatives qui correspondent aux besoins des programmes et tiennent compte de la participation des utilisateurs sont les suivants :

1. Les engagements de niveaux de service pour les RL et le RE;
2. La sécurité des équipements RL/RE, des dispositifs de bureautique et des données sur les serveurs et les ordinateurs locaux;
3. La tolérance aux défaillances des RL, du RE et du courrier électronique, y compris la tolérance de points névralgiques et le besoin d'un soutien permanent;
4. Le niveau de service RL/RE pour les petits bureaux, ainsi que les sites très éloignés, y compris les navires;
5. Les critères applicables à l'évolution de la suite de bureautique, y compris le système de courrier électronique;
6. L'utilisation acceptable de l'Internet, y compris la différenciation entre l'utilisation pendant et après les heures normales de travail, et la mesure dans laquelle le MPO servira de fournisseur général de services Internet auprès de son personnel;
7. L'utilisation de modems configurés pour répondre automatiquement sur les ordinateurs de bureau connectés au RE;
8. Les conditions en fonction desquelles un RL peut être établi pour répondre aux besoins des programmes;
9. Les règles applicables aux systèmes coupe-feu ministériels;
10. L'emplacement de tous les dispositifs de réseau et la fourniture d'alimentation ininterruptible et de secours;
11. L'étendue et la nature du soutien en dehors des heures normales de travail;

12. Les règles d'affectation pour l'accès à la largeur de bande, y compris une définition des circonstances dans lesquelles l'utilisation de la largeur de bande sera facturée aux secteurs de programmes;
13. Le traitement salarial cohérent du temps consacré aux activités du MPO sur un ordinateur ministériel relié au réseau ministériel en dehors des heures normales de travail;
14. L'identification des dispositifs informatiques de poche acceptables, des plates-formes soutenues et des utilisations soutenues;
15. L'identification des types d'information qui peuvent être diffusés sur l'Internet et l'Intranet, et des types d'information qui ne doivent pas être diffusés de cette façon;
16. L'identification claire des types d'information qui peuvent être distribués par courrier électronique de masse, et des circonstances et mécanismes d'adressage du courrier électronique à large diffusion uniquement aux employés pour qui cette information est pertinente.

L'absence de conseils et d'orientations clairs s'étend à l'acquisition de matériels et de logiciels commerciaux, ainsi qu'au développement de systèmes personnalisés. Dans le sondage des utilisateurs réalisé dans le cadre de cet examen, une question portant sur « les ressources étudiées ou consultées avant d'acquérir un nouveau matériel informatique ou logiciel » permettait d'identifier de multiples ressources. Seulement 30 % des personnes ayant des pouvoirs d'achat disaient consulter le document sur l'architecture informatique du MPO, le Bureau d'assistance ou le personnel de la DGGIST avant de faire une acquisition, 38 % disaient consulter des articles dans des revues informatiques, tandis que 72 % disaient consulter un collègue bien informé. Dans les Maritimes et la région Laurentienne, on encourage fortement les responsables à utiliser le rigoureux processus de planification élaboré pour le MPO par DMR avant d'entreprendre un projet de développement d'application personnalisée. Même là, les projets entrepris dans les secteurs de programmes n'utilisent souvent qu'une portion du processus DMR.

L'exploitation du système RL/RE présente aussi de larges variations en termes de mise en œuvre et de fonctionnement. Par exemple, dans certaines régions, un contrôle très serré de l'accès à l'Internet fait contraste avec les contraintes très limitées imposées dans d'autres régions. De même, il continue à y avoir des propositions visant l'établissement de RL et de RE entièrement internes aux secteurs de programmes (par exemple, INNAV, une récente initiative de la Garde côtière qui est encore en développement). Si ces projets étaient réalisés, il s'ensuivrait que le même équipement exploitant le même logiciel pour réaliser le même objectif d'interconnexion serait mis en œuvre par deux organisations parallèles du même ministère.

Même les sérieuses lacunes de formation identifiées par le sondage des utilisateurs (40 % du personnel du MPO veut obtenir de la formation sur les TI) peuvent être attribuées à l'absence d'une politique exigeant la mise en œuvre intégrée de nouveaux logiciels et systèmes. Cette intégration devrait comprendre de la formation obligatoire, ainsi qu'une évaluation des problèmes de réseau qui pourraient survenir. Des problèmes de formation ont été associés au récent déploiement partiel d'Office 97 (25 % du personnel du MPO continue à souhaiter de la formation sur la suite de bureautique). Cette opération a également connu des problèmes de compatibilité des matériels. La région Laurentienne, probablement l'une des principales bénéficiaires du soutien supplémentaire des outils bilingues de la suite Office 97, n'a pu offrir ce produit qu'à la moitié

seulement de ses utilisateurs, à cause des contraintes matérielles. De plus, l'incompatibilité des fichiers Office 97 et de la version précédente a été identifiée par les utilisateurs comme un problème majeur associé à ce changement.

3.4.2 Souhaitable ou nécessaire

Grâce au service de marketing de Microsoft, presque tout le monde en Amérique du Nord reconnaît le slogan « Où voulez-vous aller aujourd'hui? ». Dans un contexte informatique d'affaires, cependant, un credo plus pertinent serait « Où ***devez-vous*** aller aujourd'hui? ». Le MPO applique les deux modèles, le premier étant plus coûteux, tandis que le second convient mieux à cette époque de modération des dépenses. L'examen de la DGGIST réalisé en 1994 par Price Waterhouse indiquait clairement que « la solution [à ce trop grand nombre de projets à demi exécutés ou pas commencés] devrait être d'en faire moins, plutôt que de continuer à jongler avec des demandes de ressources conflictuelles ».

Le MPO, par le processus d'architecture informatique, a entrepris l'harmonisation complète et nécessaire de ses matériels et logiciels. Si le temps s'était arrêté, cela aurait été presque suffisant. Nous avons commencé par un environnement pour « groupes de travail » (où de petits groupes d'employés partageaient de l'information et choisissaient différents systèmes de traitement de texte, différents systèmes d'exploitation et différents systèmes de courrier électronique). Nous sommes maintenant passé à un modèle « entièrement intégré » (où les communications ministérielles sont facilitées par une norme bureautique pour le partage de fichiers, un seul système d'exploitation de réseau et un seul système de courrier électronique.)

La rentabilité de la micro-informatique, par rapport à presque n'importe quel autre groupe de produits, découle uniquement de l'implantation de normes fortes. Quand le public a choisi de voir le système de bureautique IBM comme une norme dans un environnement extrêmement disparate, la micro-informatique a connu une croissance phénoménale. En moins de vingt ans, les ventes de micro-ordinateurs sont passées de zéro à 200 millions d'unités par année. Comme le soulignait Bill Gates en 1998, lors de son témoignage devant le Sénat américain pour se défendre contre des accusations selon lesquelles Microsoft recourait à des méthodes monopolistes, si les coûts et la performance des avions avaient suivi la même courbe prix-performance que l'informatique, « un 747 ne coûterait pas plus cher qu'une pizza ». Les normes ont été la clé de l'efficience et de la concurrence des prix, et elles offrent au MPO la possibilité d'être efficient et rentable dans le domaine des TI.

La question clé est la suivante : comment le MPO devrait-il établir des normes afin de s'aligner clairement sur les besoins des programmes et les contraintes financières actuelles? Il peut être utile pour nous de considérer ce qui est nécessaire d'abord, et ce qui pourrait être souhaitable plus tard. Le MPO pourrait bénéficier grandement d'une évolution utilisateur-fournisseur de la norme d'architecture informatique. Nous travaillons maintenant dans un environnement qui comprend des ordinateurs de poche, des communications numériques internationales par satellite et des implantations sophistiquées des multimédias. Aucun de ces éléments n'est pris en compte dans le document sur l'architecture, mais ils existent tous maintenant sous diverses formes au sein du MPO.

3.4.3 L'évolution de la suite de bureautique standard

Dans le cadre du processus d'architecture informatique, il a été décidé d'adopter la suite de produits Microsoft Office. Cette décision émanait d'un processus qui tenait compte non seulement de la compatibilité des matériels, mais comprenait aussi des consultations auprès des clients de tous les secteurs. Tel qu'indiqué ailleurs dans ce rapport, cette approche est considérée comme une « pratique optimale ».

La modification suivante du bureau standard, qui s'est faite à la grandeur du Canada, a été traitée différemment. En 1998, la suite de bureautique a été mise à niveau, passant de Office 4.3 à Office 97. Cette nouvelle version est devenue la norme nationale du MPO, même si aucun dossier justificatif n'avait été préparé pour en démontrer les avantages supplémentaires, et même si l'information d'inventaire indiquait qu'un nombre important d'utilisateurs seraient dans l'impossibilité d'adopter la nouvelle norme en raison de la mémoire limitée et de la lenteur des processeurs de leurs PC. En outre, les clients n'ont pas été consultés sur le besoin de capacité accrue que la suite Office 97 pourrait créer. Seuls les utilisateurs qui avaient des ordinateurs suffisamment puissants ont reçu Office 97, et les autres, qui ont continué à se servir d'Office 4.3, se sont retrouvés avec des problèmes d'incompatibilité avec les autres utilisateurs du MPO. L'évaluation actuelle d'Office 97, qui ne fonctionne pas bien sur des ordinateurs 486, couplée aux coûts associés à la mise à niveau des matériels, indique que cette situation persistera jusqu'à ce que tous ces ordinateurs soient remplacés. Durant les entrevues et les discussions, nous avons appris qu'il était fréquent que les employés du MPO reçoivent des fichiers Word, Excel et PowerPoint incompatibles. Une solution intérimaire pour la gestion de cette incompatibilité existe et devrait être mise en œuvre.

Le retour au modèle du dossier justificatif utilisé lors de l'élaboration du document sur l'architecture informatique est important, car Microsoft continue de faire évoluer sa suite de bureautique et vient de lancer la version préliminaire d'Office 2000. Le MPO doit faire en sorte que les futurs changements apportés à la suite de bureautique ministérielle ne soient faits qu'après l'élaboration d'un dossier justificatif complet. Office 2000 applique le paradigme Internet à toutes les fonctions de bureautique importantes. Chaque ordinateur relié au réseau peut « publier » sous forme de pages Web des documents, des rapports, des feuilles de calcul et des présentations. Il s'agit certainement d'un changement majeur, qui devrait faire l'objet d'une analyse justificative complète, tenant compte des besoins des utilisateurs, ainsi que des répercussions sur les matériels et la sécurité.

Il peut arriver, dans certains cas, qu'un groupe de personnes collaborant à l'élaboration de documents utilisent une norme de document différente de la norme ministérielle. C'est souvent le cas dans le secteur des Sciences, où les collaborateurs appartiennent souvent à d'autres institutions scientifiques. Et cela peut être une explication plausible des résultats du sondage indiquant qu'on trouve Lotus Word Pro et WordPerfect sur certains ordinateurs du MPO. Il est clair qu'une approche ministérielle basée sur l'interopérabilité reconnaîtrait que la norme ministérielle doit s'appliquer à l'intérieur du MPO et que, si d'autres normes sont appropriées, le personnel du MPO

devrait avoir accès à d'autres produits de bureautique, ou à d'autres version
Microsoft, pour bénéficier d'un niveau d'interopérabilité acceptable avec le

3.4.4 Internet – « Où puis-je aller aujourd'hui? »

Dans cet examen, nous avons comparé les nouvelles approches basées sur l
approches moins technologiques, afin d'évaluer la gestion des nouvelles ap
celle des anciennes méthodes. Cette comparaison est très difficile à faire p
l'ensemble de cette section, toutes les références renvoient à l'Internet, et n
gouvernemental interne appelé l'Intranet. Bien que l'Intranet présente de n
avec son cousin géant l'Internet, du point de la sécurité, ce sont deux mond

Pour commencer, il importe de noter que nous avons été dans l'impossibili
analyse ou un dossier justificatif appuyant la fourniture de l'accès Internet
employés du Ministère. Il existe d'autres institutions fédérales aussi grande
MPO (comme Revenu Canada) où l'accès Internet complet n'est pas fourni
Certains utilisateurs du MPO, particulièrement dans le secteur Sciences, ut
l'Internet depuis sa création.

D'une certaine façon, l'équivalent « non TI » de l'Internet est une bibliothè
un accès direct ou indirect à toutes sortes d'information. Il est instantané,
bidirectionnel. En outre, il est possible pour les sites Web de déterminer qu
d'obtenir de l'information technique sur les ordinateurs de leurs visiteurs.
employé visite une bibliothèque du MPO (les bibliothèques étaient les seul
d'information généralement offertes aux employés ministériels avant l'exis
trouve une collection de ressources soigneusement sélectionnées qui se rap
MPO ainsi que des sources d'information générale comprenant les journaux
l'accès Internet à tous ses utilisateurs, le MPO a mis à leur disposition un é
beaucoup plus large.

Le Secrétariat du Conseil du Trésor (SCT) est au fait de cet éventail de ress
politique générale d'utilisation acceptable, qui recommande que les différe
des politiques correspondantes se rapportant plus spécifiquement à leur situ
exige des vérifications périodiques de la mise en œuvre ministérielle, ce qu
au MPO.

En l'absence d'une politique ministérielle approuvée, le MPO n'a pas surv
qui sont visités par ses utilisateurs. En outre, bien qu'il soit possible de « b
certains sites, à l'heure actuelle, seulement trois systèmes coupe-feu sont é
de blocage. Dans tous les cas, la seule utilisation qui est bloquée est l'audi
multimédia. Ce choix semble contradictoire, cependant, avec la transition
bureautique ministérielle à des ordinateurs équipés de cartes son et de haut
régions et dans la RCN, où ce blocage multimédia a été instauré, les utilisa
avertis de ce changement (la quatrième région où le blocage est en vigueur
a averti tous ses utilisateurs). On a fait ce choix en sachant pertinemment

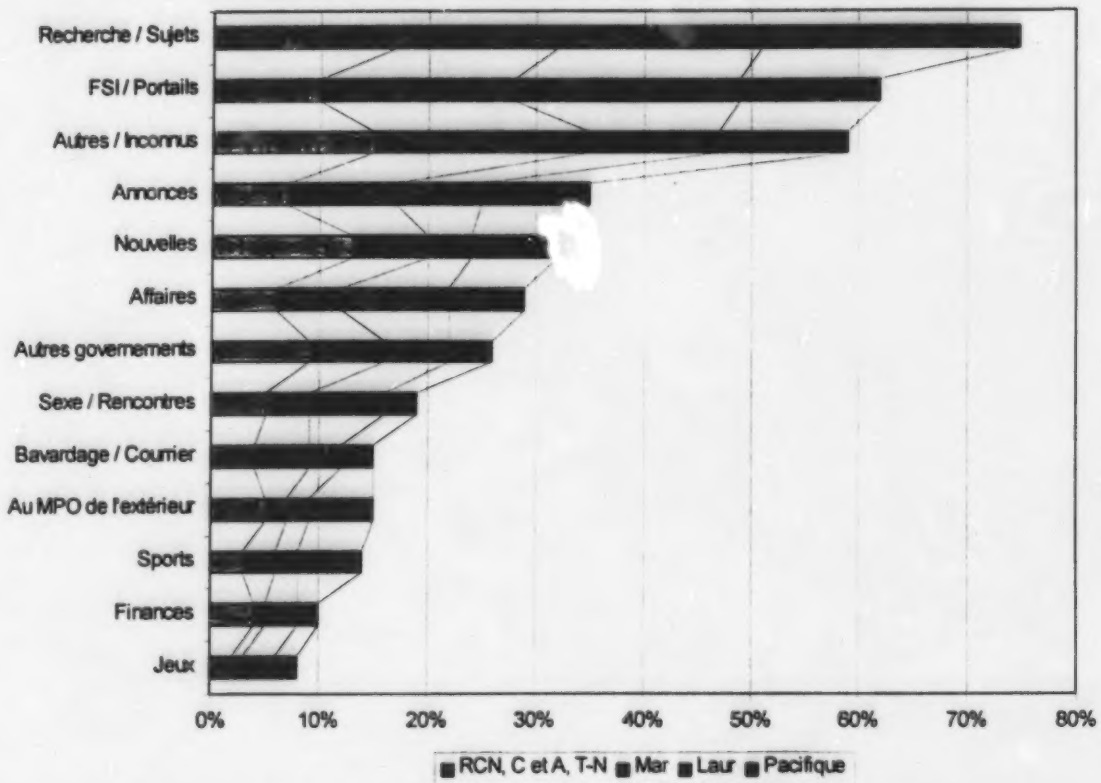
nordiques éloignés se verraient privés de leur seul accès à la radio de la CBC/SRC et que certains employés de la RCN surveillaient la radio locale dans les communautés côtières. Ce blocage a été instauré pour réduire la charge sur les liaisons réseau entre Terre-Neuve et la RCN, alors que le trafic à d'autres sites qui n'ont clairement rien à voir avec les activités du MPO demeure ouvert.

Signalons une autre incohérence reliée à l'Internet. Bien que tous les utilisateurs du MPO aient accès à l'Internet depuis leur poste de travail, les utilisateurs de la RCN et des Maritimes qui accèdent à l'ordinateur du MPO à partir de sites éloignés ont accès à toutes les ressources ministérielles, y compris l'Intranet, mais l'accès à l'Internet leur est complètement bloqué (à moins qu'une entente d'utilisation spécifique soit signée). Le personnel ministériel à Terre-Neuve, et dans les régions du Centre, de l'Arctique et du Pacifique qui accèdent au réseau du MPO ont un accès complet à l'Internet. Cette différence n'est basée sur aucune politique. On craint que les employés du MPO qui se connectent à partir de leur domicile utilisent le MPO de la même manière qu'on utiliserait un fournisseur commercial de services Internet. Il n'existe aucune politique ministérielle stipulant que cette utilisation est inacceptable.

Une analyse complète de l'utilisation de l'Internet par le personnel ministériel de toutes les régions indique qu'au moins 10 % du trafic Internet vise des sites qui n'ont absolument rien à voir avec les activités de travail. Pour chacun des quatre systèmes coupe-feu qui gèrent l'accès Internet, l'utilisation a été répartie en 13 catégories, qui sont définies et décrites ci-après.

Au MPO à partir de l'extérieur	Un site du MPO : Garde côtière canadienne, Institut des sciences de la mer, etc. Comme il s'agit du trafic géré par le système coupe-feu, seul le trafic venant de l'extérieur est indiqué ici. Les visites par le personnel du MPO à l'Intranet du MPO ne peuvent être contrôlées que sur les 30 serveurs Web utilisés à cette fin.
Autres sites gouvernementaux	Autres sites fédéraux et provinciaux : Conseil national de recherches du Canada, DRHC
Recherche / sujets	Sites de recherche et portails : AltaVista, MSN
Activités opérationnelles	Sites reliés aux activités ministérielles : Cambridge Scientific, ZiffNet
Nouvelles	Sources de nouvelles : Canoe, sites de journaux
Finances	Sites de banques, marchés boursiers
Bavardage/courriel	Hotmail, Yahoo Chat
Annonces	Annonces à double-clic
Sports	Site de la LNH, sites de football et de baseball
Sexe / Rencontres	US Date, [illegible]eteen.com
Jeux	Jeux informatiques et autres; site Sony Playstation
FSI / Page d'accueil	Ces sites correspondent à des pages d'accueil d'utilisateurs ou autres, et il est impossible d'identifier les sites visités car de nombreux sites sont hébergés dans ses sites généraux. Le site du FSI « Geocities » revient très fréquemment, car c'est un site où l'on peut trouver des fichiers de musique (MP3).
Autres / inconnus	Les sites dont il est impossible de déterminer le contenu; pas de consultation inversée et/ou la page d'accueil ne contient pas d'information sur le site ou de liens. Exemple : 209.143.228.181

Tableau 3.4.4.1 Une semaine de trafic Internet par système coupe-feu (accès par ETP par jour, par catégorie)



Ce graphique indique clairement que les visites à des sites gouvernementaux sont rares, comparées aux recherches généralisées et aux « inconnus » (pour des raisons techniques, cette catégorie ne comprend pas de sites gérés par les gouvernements fédéral et provinciaux). Il indique aussi qu'une proportion d'environ 10 % du trafic vise des sites sans lien apparent avec les activités de travail. L'utilisation moyenne réelle de l'Internet a été évaluée comme le nombre moyen d'accès Internet par ETP par jour. Ces données sont présentées dans le tableau suivant :

Région	Accès Internet par ETP par jour
Maritimes	28,5
Terre-Neuve	28,9
RCN	
Centre et Arctique	
Laurentienne	42,2
Pacifique	67,0

Il faut souligner que les utilisateurs qui communiquent par modem avec le MPO à partir de leur domicile dans la RCN et les Maritimes n'ont pas accès à !'Internet, mais que les utilisateurs qui ont le même type d'accès ministériel dans la région du Pacifique, la Laurentienne et Terre-Neuve ont l'accès complet à l'Internet. Étant donné que le RE, les RL et les coupe-feu indiquent un faible niveau d'utilisation en dehors des heures normales de travail et que l'accès Internet est facturé au MPO sur une base forfaitaire, il n'est pas possible d'identifier les coûts associés à l'utilisation de l'Internet par les utilisateurs qui s'y connectent de leur domicile. Il y aurait des coûts potentiels si des « ports » de connexion commutée supplémentaires étaient nécessaires pour obtenir cet accès Internet à domicile. La région du Pacifique compte moitié moins de ports de connexion par ETP que la RCN, et deux fois plus d'utilisation Internet, de sorte que rien n'indique que des ports supplémentaires ont été installés pour fournir l'accès Internet aux utilisateurs du MPO à partir de leurs ordinateurs domestiques. L'ébauche de politique d'utilisation acceptable de l'Internet, qui est en voie de révision, ne fait aucune distinction entre l'utilisation de l'Internet au moyen d'une connexion directe du poste de travail et l'utilisation de l'Internet par accès commuté par modem.

Les dépenses directement reliées à la fourniture de l'accès Internet sont faibles comparées à l'ensemble des dépenses ministérielles. Il faut toutefois noter que l'engorgement de la liaison RE entre le MPO et le reste du Ministère était, selon le personnel de la DGGIST, causé par l'utilisation soutenue de l'Internet, et que cette utilisation était reliée aux procédures de destitution du président américain. Il est donc important de souligner que l'accès Internet sur le RE et les RL du MPO peut effectivement être un article de dépense. L'utilisation de sites « non reliés au travail » durant ou après les heures de travail n'était pas un article de dépense important durant la période qui a été contrôlée pour cet examen. Il semble cependant y avoir des problèmes de gestion (salaires, charge de travail) qui se rapportent à la productivité générale au sein du Ministère. Durant la réalisation de cette évaluation, aucune utilisation criminelle de l'Internet n'a été détectée.

3.4.5 Accès à partir de sites éloignés

Le MPO a besoin de la connectivité à distance pour diverses raisons, y compris l'accès sécurisé pour les bureaux éloignés, les navires, les télétravailleurs à domicile, les employés qui voyagent et doivent accéder aux services de courrier électronique et les employés qui travaillent à domicile en dehors des heures normales de travail. Tel qu'indiqué dans le sondage des utilisateurs, environ 2 520 personnes accèdent au réseau du MPO de l'extérieur du bureau. De ce groupe, 650 personnes accèdent au réseau à partir d'un ordinateur domestique appartenant au MPO.

Le sondage des utilisateurs indiquait que 65 % des utilisateurs d'accès à distance étaient satisfaits de ce service et que 62 % d'entre eux estimaient que le service était fiable. Dans l'ensemble, bien que la différence soit petite, les répondants ont évalué la facilité d'utilisation de l'accès à distance de façon légèrement plus favorable que la fiabilité du logiciel de connexion/d'accès. La cote moyenne de la facilité d'utilisation, sur une échelle de 5 points, était de 3,84, comparée à une cote moyenne de 3,71 pour la fiabilité. Dans l'ensemble, ce sont des cotes positives indiquant que l'accès à distance fonctionne généralement bien. En moyenne, les répondants de la région du Pacifique ont accordé à la fiabilité la cote la plus basse. Le secteur de la Gestion des pêches et le secteur des Sciences ont accordé la cote la plus faible à la facilité d'utilisation et le secteur de la Gestion des pêches a également attribué la cote la plus faible à la fiabilité.

L'accès à distance est fourni de façon différente d'une région à une autre. La connectivité et la vitesse de l'accès à distance varient considérablement à l'échelle nationale et à l'intérieur des régions. Il n'existe aucune politique qui détermine qui peut avoir accès (ou ne pas avoir accès) à des lignes RNIS de grande capacité (réseau numérique à intégration de services); cela se fait à la discrétion de la DGGIST, même si celle-ci ne finance pas ces lignes. Un examen des pratiques de gestion régissant l'accès à distance a permis de constater que la tenue de dossiers n'est pas fiable. Dans certains cas, les employés sont tenus de remplir des formulaires, tandis que dans d'autres cas, il n'existe aucune autorisation imprimée ou électronique. La comparaison des dossiers d'accès à distance pendant un mois et des formulaires d'approbation a confirmé que la gestion de ces dossiers est inégale et que les contrôles ne sont pas visibles. Comme nous l'avons indiqué dans la section portant sur l'Internet, l'accès Internet à partir des sites éloignés n'est pas traité de façon cohérente. Il faut donc préciser les politiques, les procédures, les rôles et les responsabilités en matière d'accès à distance.

La gestion des micro-ordinateurs ministériels utilisés à domicile par des employés est, elle aussi, inégale. Tel qu'indiqué ci-dessus, le sondage des utilisateurs indiquait qu'environ 650 personnes travaillent à domicile après les heures normales de travail sur des ordinateurs qui appartiennent au Ministère. L'examen de la documentation sur les utilisateurs de connexions commutées n'a pas permis de déterminer si ces personnes avaient conclu une entente de télétravail avec le MPO. Un problème général de gestion causé par les TI est le traitement différentiel du travail supplémentaire à partir de ces ordinateurs domestiques. Il n'est pas clair si la fourniture d'un ordinateur ministériel (non en surplus) à un membre du personnel constitue une « autorisation » implicite de travail supplémentaire ou une forme quelconque d'avantage accessoire. Il n'est pas clair si les postes de travail appartenant au MPO sont une forme de télétravail (rémunéré ou non).

Il y a très peu de « télétravail » explicite au sens où un employé individuel renonce à un bureau et travaille pour le Ministère durant les heures normales de travail à partir de son domicile. Les quelques « télétravailleurs » qui existent actuellement utilisent généralement cette approche en raison de problèmes de santé et pour des périodes de moins d'un an. Étant donné les contraintes financières du Ministère ainsi que la souplesse que procure le télétravail (aucun espace de bureau n'existe officiellement pour l'employé télétravailleur), une gestion plus claire de cette possibilité reliée aux TI est souhaitable.

3.5 SÉCURITÉ

3.5.1 Évaluation de la menace et des risques

Durant la réalisation de cette étude, la Garde côtière canadienne a commandé une étude sur les communications réseau sécurisées. Même si la portée de cette étude se limitait au secteur de la Garde côtière et que l'analyse était en grande partie inférentielle, cette étude et l'évaluation connexe de la menace et des risques constituent une indication utile de la nature et des incidences des menaces pour le système de RE/RL du MPO. Les résultats de cette étude ont été fournis au consultant chargé d'analyser le RE et les RL pour cet examen. Dans l'ensemble, plusieurs points

d'action ont été identifiés. Les secteurs de risque qui nécessitent une intervention urgente sont identifiés dans les sous-sections suivantes.

3.5.1.1 Architecture des liaisons Internet

Une grande priorité a été attribuée à la conformité An 2000 pour faire en sorte que les systèmes essentiels du MPO demeurent opérationnels. Cependant, il est également important de s'assurer que notre réseau est aussi protégé contre d'autres menaces plus imminentes, spécialement en provenance de l'Internet. L'analyse indique que certaines menaces graves pourraient découler de la façon dont l'accès à destination et en provenance de l'Internet est configuré. Bien qu'il permette d'accéder rapidement à une grande variété de services d'information et qu'il ait permis aux communications écrites (courrier électronique) d'être aussi rapides et universelles que le téléphone, l'Internet est un environnement très dangereux. Nos interfaces avec l'Internet (systèmes coupe-feu) sont gérées de façon inégale et en l'absence de politiques et règles claires. L'effet net de cet état de choses, c'est qu'il existe des ensemble de règles « plus permissives » et d'autres « moins permissives » qui régissent le trafic Internet. Étant donné la nature du RE et des RL, le coupe-feu le moins permissif établit le niveau de risque pour l'ensemble du système, même s'il y a six coupe-feu au MPO. La gestion efficace de cet aspect des TI nécessite, encore une fois, l'application de l'approche du « dossier justificatif », comme elle le fait ailleurs. Il y a certes des utilisateurs qui sont habitués à des échanges largement sans contraintes avec des utilisateurs de l'extérieur sur l'Internet. Une telle analyse de dossier justificatif permettra d'évaluer comment répondre le mieux aux besoins tout en réduisant les risques pour l'ensemble du réseau.

L'architecture du système de courrier électronique est également très exposée aux risques posés par l'Internet. Le système existant comporte certaines installations où tout le courrier, d'où qu'il provienne, est envoyé à des serveurs situés à l'intérieur du système coupe-feu. Sur l'Internet, il est facile de trouver des outils simples qui peuvent servir de « lettres piégées » capables de saboter des serveurs de courrier entiers. Si le courrier électronique provenant de l'Internet était traité sur un serveur distinct (habituellement hors de la zone protégée), le courrier interne du MPO pourrait alors survivre à une attaque provenant de l'Internet. Dans certaines régions (comme les Maritimes), le système coupe-feu bloque le courrier à problème (c.-à-d. le courrier non sollicité et la publicité importune). Cette approche n'est pas mise en application sur le serveur de la RCN, qui accepte tout le courrier, y compris le courrier à relayer.

Pour que le MPO puisse continuer à mener ses affaires électroniques sans interruption, l'équipe d'examen recommande la réalisation d'une évaluation détaillée de la menace et des risques visant spécifiquement l'accès Internet et la configuration des systèmes de courrier électronique.

3.5.1.2 Information protégée et sensible

L'équipe d'examen n'a trouvé aucun programme systématique informant les utilisateurs du niveau de sécurité de l'information électronique et du courrier électronique enregistré. Le sondage réalisé dans le cadre de cet examen indiquait que, de tous les services partagés, le plus apprécié est le courrier électronique. Dans de nombreux secteurs clés, le courrier électronique a complètement remplacé le système de correspondance imprimée pour les communications internes. Bien

qu'aucune étude du contenu du courrier ou des fichiers électroniques n'ait été réalisée, il existe un risque que de l'information sinon secrète, du moins sensible (mesures d'application de la loi, information sur le personnel, etc.) réside sous forme d'enregistrements électroniques dans le système du MPO. Durant la réalisation de cet examen, la Garde côtière canadienne a commandé une étude de sécurité complète qui a permis que constater que l'information circulant dans le système de courrier électronique actuel peut être interceptée et modifiée.

La gestion de l'utilisation du courrier électronique, maintenant qu'il s'agit du système de communication le plus courant au Ministère, nécessite la réalisation d'une évaluation complète de la menace et des risques. Bien que nous n'ayons trouvé aucune indication que de l'information secrète ou très secrète ait été transmise par courrier électronique, il est certain que de l'information sensible a été transmise. Les quatre catégories de sensibilité de l'information sont :

1) Très faible - Information qui, si elle est compromise, n'est pas susceptible de causer des préjudices hors de l'intérêt national (NON CLASSIFIÉE);

2) Faible - Information qui, si elle est comprise, pourrait être susceptible de causer des préjudices hors de l'intérêt national (PROTÉGÉE A);

3) Moyenne - Information qui, si elle est compromise, pourrait être susceptible de causer des préjudices graves hors de l'intérêt national (PROTÉGÉE B) et

4) Élevée - Information qui, si elle est compromise, pourrait être susceptible de causer des préjudices exceptionnellement graves hors de l'intérêt national (PROTÉGÉE C) et information qui, si elle est compromise, pourrait être susceptible de causer des préjudices à l'intérêt national (CLASSIFIÉE).

Le consultant engagé par la Direction générale de l'examen pour ce volet des travaux a évalué que notre réseau était sécurisé jusqu'au niveau Protégé A, tel que prévu dans la conception du réseau. Une étude plus poussée pourrait examiner cette question de façon plus détaillée, mais, durant les discussions que nous avons eues avec le personnel du MPO, il est devenu évident qu'il n'y avait aucune compréhension de la « limite » de la sensibilité de l'information qui pouvait être transmise par des moyens électroniques. Nous avons des raisons de croire que de l'information de niveau Protégé B (qui comprend l'information qui pourrait être embarrassante pour le Ministère ou l'information sensible sur les activités, le personnel ou les programmes du Ministère) est transmise sur l'actuel système de courrier électronique. Il existe des solutions techniques (voir les sections 3.5.3 et 3.5.4), mais elles sont coûteuses et demanderaient du temps. Une première mesure efficace serait d'informer le personnel que le courrier électronique ne devrait pas être utilisé pour transmettre de l'information sensible, ce qui comprendrait, par exemple, des messages de courrier électronique contenant des numéros de cartes de crédit et les noms des utilisateurs autorisés de ces cartes.

3.5.1.3 Accès par d'autres personnes que le personnel ministériel

Le RE et les RL du MPO comptent trois groupes distincts d'utilisateurs « non ministériels ». Le premier groupe est composé des entrepreneurs et des étudiants, ainsi que des autres personnes qui, durant leur séjour au MPO, se voient attribuer des noms d'utilisateurs et le type d'accès spécifié par le superviseur ou le client du MPO. Dans ce cas, le principal risque se rapporte à la fermeture de ces comptes quand l'accès n'est plus autorisé.

Le deuxième groupe est constitué des employés d'autres ministères qui travaillent dans les immeubles du MPO. Le Ministère le plus présent est Ressources naturelles Canada, bien que le personnel d'Agriculture et Agro-alimentaire Canada ait également accès. Les employés de Ressources naturelles Canada (RNCan) travaillent, pour la plupart, à l'Institut océanographique de Bedford et à l'Institut des sciences de la mer. À l'Institut océanographique de Bedford, ces employés désiraient un accès Internet plus ouvert que celui permis par la DGGIST des Maritimes et l'on a résolu cette question en permettant aux employés de RNCan d'avoir leur propre accès Internet, mais aucun accès au RE et aux RL du MPO. À l'Institut des sciences de la mer, cependant, des modifications permissives ont été apportées aux règles applicables au système coupe-feu et ces changements créent un certain risque pour le RE et les RL. Si les employés d'autres ministères fédéraux estiment avoir besoin d'un accès plus large que celui qui est permis par le MPO à son propre personnel, alors il est clair qu'un dossier justificatif devrait être préparé, et que les risques et les avantages doivent être explicitement évalués. L'examen n'a trouvé aucun dossier justificatif de ce genre.

Le troisième groupe d'utilisateurs non ministériels se trouve au Collège de la Garde côtière canadienne. Le Collège forme maintenant des étudiants qui viennent du monde entier. Dans le cadre de leur travail, ils utilisent l'infrastructure de TI du MPO dans les salles de cours supervisées et, sans surveillance, dans les aires communes et les résidences pour étudiants. Bien qu'il y ait un système coupe-feu entre le Collège de la Garde côtière et le RE/RL du MPO, ce système sert actuellement à limiter le trafic provenant du RE du MPO vers le Collège, au lieu d'être utilisé pour limiter l'accès depuis l'intérieur du Collège. Le Collège de la Garde côtière exploite également un coupe-feu Internet et a mis en application des règles qui permettent l'accès illimité vers l'extérieur, mais restreignent sévèrement le trafic qui arrive. En outre, l'architecture du courrier électronique de la Garde côtière est conservatrice et résistante à certains des risques qui sont évidents dans d'autres parties du RE/RL. La raison donnée pour l'installation d'un coupe-feu entre le Collège de la Garde côtière et le reste du MPO était que le RE et les RL actuels n'étaient pas suffisamment protégés contre les intrusions.

3.5.1.4 Modems à réponse automatique

Les employés du MPO utilisent depuis un certain temps des ordinateurs pour travailler à domicile. Avant les réseaux bien établis et le type d'accès téléphonique rapide maintenant accessible, les employés du MPO qui souhaitaient travailler chez eux pouvaient appeler leur ordinateur ministériel à partir d'un ordinateur domestique (ou d'un autre site éloigné, comme une station locale ou un hôtel) et établir une connexion directe entre les deux ordinateurs. Cela se faisait à

l'aide d'un dispositif appelé modem (**mo**dulateur/**dém**odulateur) qui permettait à l'ordinateur ministériel de « répondre » à l'appel entrant et de donner à l'utilisateur éloigné l'accès à son propre ordinateur ainsi qu'au réseau du MPO. Dans l'environnement actuel, avec l'accès commuté fiable et rapide et le courrier électronique Internet, ces modems sont moins nécessaires. Néanmoins, quand ces modems sont laissés en marche après les heures normales de travail et sont protégés par des systèmes de sécurité inadéquats, ils peuvent constituer un moyen pour des utilisateurs non autorisés d'accéder au RE et aux RL du MPO. Il existe des configurations de sécurité (par exemple, une procédure de rappel, où le modem appelle un seul numéro de téléphone qui est celui de l'emplacement autorisé de l'utilisateur), mais aucune politique n'exige ce type de configuration. Pour gérer ce risque, on peut effectuer un simple test. La première étape à suivre pour identifier le nombre de modems à réponse automatique existant sur les lignes téléphoniques du MPO serait d'appeler toutes les lignes du MPO après les heures normales de travail pour détecter les lignes qui répondent par un signal d'établissement de liaison. Une fois que cette liste de lignes téléphoniques à réponse automatique aura été créée et qu'on en aura éliminé les télécopieurs, il sera alors possible d'identifier les utilisateurs de ce type d'accès commuté, et l'on pourra prendre les mesures nécessaires pour s'assurer qu'une sécurité adéquate est en place. Lors d'une récente réunion de l'Institute of Internal Auditors, ces modems à réponse automatique ont été identifiés comme le risque de sécurité le plus grave pour le système bancaire international.

3.5.2 Sécurité physique des actifs et de l'information

Le processus à suivre pour assurer la sécurité physique des actifs de TI est le même que celui qu'on utilise pour les autres actifs importants du Ministère, à une particularité près, c'est-à-dire que les ordinateurs (y compris les serveurs et les postes de travail) peuvent être presque immédiatement démontés en pièces détachées qu'il est alors impossible de distinguer de composantes neuves. Un autre aspect plus important est que l'information qui réside dans l'ordinateur pourrait être perdue à jamais si une copie de sauvegarde n'est pas conservée sur bande ou sur le réseau. Il existe un autre risque, qui concerne les ordinateurs qui jouent un rôle important dans le réseau (les serveurs, les routeurs, les serveurs de noms, etc.) et qui contiennent de l'information susceptible d'être utile à ceux qui désirent s'infiltrer dans le RE et les RL du MPO.

Le MPO s'est déjà fait voler de l'information et des ordinateurs. Dans un cas, lors de son départ du MPO, un employé a pris une bande de données sur les prises, qu'il a ensuite utilisée pour lancer une entreprise de consultation. Selon les lois sur le droit d'auteur en vigueur à ce moment-là, il s'est révélé que le seul crime commis était le vol de la bande elle-même, estimée à moins de 50 $. Dans d'autres cas, des ordinateurs de bureau et des puces de mémoire ont été volés. Selon le personnel responsable de la sécurité, le vol de puces de mémoire était un problème sérieux il y a trois ans, mais que ce n'est plus le cas aujourd'hui, probablement à cause de la réduction des prix de la mémoire informatique, plutôt qu'à cause d'un renforcement de la sécurité physique. Il est également arrivé que des ordinateurs soient endommagés ou détruits, lorsque les bureaux du MPO ont été occupés par des manifestants.

La plupart des équipements du RE et des RL sont conservés dans des salles d'ordinateurs verrouillées avec serrures à combinaison. Bien que ces dispositions semblent sûres, il arrive souvent que les murs de ces salles soient faits de panneaux de gypse faciles à enlever. La plupart

des grands bureaux du MPO sont équipés de caméras vidéo qui surveillent les entrées et les sorties. Cela n'empêche pas le vol, mais peut servir de dissuasif pour certains cambrioleurs. En 1996, la salle des serveurs d'un autre ministère fédéral (dans les Tours Journal situées en face de l'Administration centrale du MPO, au 200 rue Kent) a été complètement vidée de ses équipements en moins de deux minutes, avec couverture vidéo complète; cependant, personne n'a jamais été arrêté.

Il est bon de concentrer les ordinateurs de réseau dans des endroits dotés non seulement d'une bonne sécurité physique mais aussi de dispositifs d'appoint appropriés (alimentation électrique, systèmes de refroidissent et systèmes de lutte contre les incendies). Étant donné la nature de la réseautique et la fiabilité générale du système téléphonique (sur lequel même le trafic réseau « interne » voyage), il serait possible de concentrer tous les équipements de réseau essentiels dans moins d'emplacements physiques que ce n'est le cas actuellement. Dans plusieurs cas, les secteurs de programmes (comme la Garde côtière canadienne, le secteur des Sciences) ont aussi leurs propres salles d'ordinateurs. Il y aurait lieu d'évaluer si la réduction du nombre de sites permettrait de réaliser des économies de coûts ou d'améliorer la fiabilité.

Pour l'instant, il ne semble pas nécessaire de renforcer la sécurité physique des ordinateurs de bureau (par exemple, en les fixant aux bureaux, en utilisant des serrures à palastre plus coûteuses). Les ordinateurs portatifs présentent un potentiel de perte de matériel ou de données pour les utilisateurs qui doivent se déplacer, mais l'équipe d'examen n'a rien trouvé qui indique que ce soit actuellement un problème sérieux pour le MPO.

3.5.3 Authentification sécurisée, chiffrement et infrastructure de clés publiques (ICP)

Le MPO évalue actuellement le besoin d'implanter des solutions de TI qui permettraient de prouver que le courrier électronique provient effectivement de l'émetteur apparent, ainsi que de façons de protéger le contenu ou d'empêcher le sabotage de l'information électronique sur le RE/RL.

Étant donné que le dossier justificatif n'a pas encore été préparé, disons seulement que les seules inquiétudes exprimées par le Secrétariat du Conseil du Trésor concernent la sécurité des transactions effectuées en vertu de la *Loi sur la gestion des finances publiques*.

Le système sur support papier que nous utilisons actuellement peut satisfaire aux exigences du CT tant que les transactions demeurent en format papier. En outre, du moment que l'accès à distance se fait par accès commuté aux dispositifs du MPO, les risques de sécurité associés à l'Internet sont évités. Bien que l'ICP soit une étape inévitable, nous pouvons l'adopter assez progressivement pour en faire une analyse exhaustive. Selon une analyse réalisée par Revenu Canada, les prix des options varient pour les cinq premières années de 3,2 millions $ à 10,1 millions $ (sur la base de 30 000 utilisateurs).

Les membres de la DGGIST des Services intégrés dans la région Laurentienne ont examiné cette question dans le contexte du MPO et leur expérience pratique pourrait probablement être utile à l'ensemble du Ministère.

3.5.6 La sécurité et l'Internet - les systèmes coupe-feu

L'Internet est un système bidirectionnel (nous pouvons obtenir de l'information de l'extérieur et, dans certaines circonstances, d'autres peuvent s'introduire dans nos systèmes s'il n'y a rien pour les en empêcher). Nous avons donc besoin d'un « garde-barrière ». Nous utilisons un système coupe-feu, c'est-à-dire un mécanisme qui protège le réseau du MPO contre les visiteurs non autorisés et qui tient un registre de l'information qui circule dans les deux sens. Le coupe-feu est essentiellement un ordinateur sophistiqué qui utilise un logiciel particulier pour remplir ces fonctions de garde-barrière.

Les systèmes coupe-feu déterminent quelles transactions peuvent franchir leurs mécanismes et ils ont la capacité de permettre à certaines choses « de sortir mais non d'entrer », et vice-versa. Dans un système où plusieurs coupe-feu jouent le rôle de garde-barrière pour le même système, il semble important que ces coupe-feu soient gérés de façon standard. Le Ministère possède six coupe-feu (Maritimes, région Laurentienne, Terre-Neuve, RCN[10], région du Pacifique et Collège de la Garde côtière). Trois d'entre eux (Terre-Neuve, RCN et région du Pacifique) sont gérés depuis Ottawa dans le cadre d'un contrat avec les SGTI, et les deux autres sont gérés localement; le Collège de la Garde côtière gère le sien. Aucun de ces coupe-feu n'utilise les mêmes règles et il n'existe pas de manuel ou de politique régissant la procédure à suivre.
La façon dont ces règles sont gérées, couplée à la façon dont les serveurs sont gérés au sein du Ministère, est importante. Deux fois en 1998, les serveurs du secteur des Sciences ont été « pris d'assaut » par une personne de l'extérieur du gouvernement, qui les a utilisés pour envoyer 33 000 messages importuns par jour. Le jour de cet incident, ce courrier représentait plus de 50 % du trafic transitant par le coupe-feu. De plus, en novembre 1998, un individu a obtenu un accès non autorisé plus large aux systèmes du MPO et leur a transmis des instructions (qui n'ont pas réussi) 300 fois en une seule journée. Les registres du coupe-feu indiquent que les tentatives d'intrusion se poursuivent. Il s'agit là d'un problème de gestion, car les SGTI reconnaissent qu'il leur incombe de surveiller les indices d'attaques en provenance de l'Internet (appelées « sondages ») et de prendre des mesures pour les bloquer; ils admettent toutefois ne pas s'occuper de cette question. Le personnel de la DGGIST de la région du Pacifique a découvert des « sondages » à l'automne de 1998 et pris les mesures nécessaires pour s'assurer que ces tentatives particulières échoueraient.

Les implications sont claires. Dans le cas des incidents de courrier importun, l'utilisateur non autorisé a réussi à accéder à un dispositif du MPO auquel il a émis l'instruction d'envoyer du courrier importun. Une fois à l'intérieur du coupe-feu, il aurait pu causer d'autres incidents plus graves (par exemple, modifier ou effacer des données, accéder à d'autres serveurs ouverts dans d'autres régions, installer un programme d'interception de messages de courrier, etc.). Ces résultats néfastes sont inévitables à moins que des mesures importantes soient prises. Ces mesures comprennent la réalisation d'une évaluation de la menace et des risques, l'élaboration d'une déclaration claire sur le niveau de risque que le système peut tolérer et une approche permettant de limiter les risques quand il est impossible d'instaurer des règles d'accès strictes pour des raisons de programmes. Les coûts que le Ministère aura à engager varieront en fonction du niveau de risque et

[10] Le trafic Internet provenant de la région du Centre et de l'Arctique, ainsi que celui des utilisateurs de Terre-Neuve qui n'appartiennent pas au secteur des Sciences, transite par le coupe-feu de la RCN.

de la période d'interruption acceptable de certaines fonctions (comme le courrier électronique) ou d'une liaison interurbaine.

À l'évidence, le Ministère a besoin d'en arriver à une entente générale sur la configuration de ces coupe-feu. L'examen des demandes de modification des règles du système coupe-feu fait également ressortir que la procédure de modification des règles est inégale. Dans le cas de deux coupe-feu (ceux de Terre-Neuve et de la RCN), il n'existe pas de piste de vérification permettant de s'assurer que l'entrepreneur (en l'occurrence les SGTI) a donné suite à ces requêtes. Il y a également trois systèmes différents en place et même les trois coupe-feu qui exploite le même logiciel utilisent chacun une version différente. Cela rend la gestion quotidienne et la coordination des coupe-feu très complexes. On prévoit convertir tous les coupe-feu au même système, mais cela n'a pas encore été fait. On envisage également de centraliser la gestion des six coupe-feu; cependant, si l'on adopte des politiques et des approches standard, il ne sera pas nécessaire, techniquement, d'éliminer la gestion régionale des coupe-feu régionaux. Il est à noter que lorsque nous avons demandé de l'information sur les règles régissant les coupe-feu, les gestionnaires régionaux des Maritimes et de la région Laurentienne nous ont répondu en une journée, tandis que les SGTI ont mis plus de deux semaines à répondre à la même requête. Il s'agit là d'un autre exemple de performance médiocre pour laquelle le contrat de 1998-1999 ne prévoyait aucun recours.

Bien qu'il soit parfois nécessaire (comme dans le secteur des Sciences) de collaborer ouvertement avec certains collègues de l'extérieur du MPO, cette collaboration doit être évaluée plus largement si elle entraîne des risques pour le RE et les RL. Les ordinateurs utilisés pour ces échanges pourraient fonctionner séparément du RE et des RL ou appliquer une méthode comme l'ICP. Dans certains cas, on pourrait poursuivre cette collaboration d'une façon qui élimine les risques pour l'ensemble du réseau.

3.6.7 Élimination des points de défaillance des systèmes essentiels

En raison de la forte dépendance des programmes envers les TI, l'interruption, même pendant quelques heures, des communications inter-bureaux ou interurbaines ou de l'accès aux applications de base (comme le courrier électronique) pourrait causer de graves perturbations. Il est essentiel de faire un effort concerté pour s'assurer que les fonctions de base sont identifiées et que les points de défaillance de ces systèmes sont éliminés, pour faire en sorte que le Ministère puisse toujours s'acquitter de ses rôles clés (par exemple, les opérations de recherche et de sauvetage, la surveillance de la trajectoire des déversements pétroliers, etc.). En ce qui concerne l'administration intégrée des systèmes de la Garde côtière, il est essentiel de souligner que bon nombre des fonctions de navigation et de recherche et sauvetage ne peuvent tolérer aucune défaillance, car ce sont des fonctions très différentes des fonctions générales de courrier électronique, de traitement de texte et de transactions financières, qui peuvent souvent tolérer un délai de 24 heures.

Le personnel technique de la DGGIST a récemment mis sur pied un groupe de travail chargé de trouver des solutions à bon nombre des problèmes techniques susmentionnés. Il s'agit là d'une excellente initiative et, avec l'inclusion du personnel de la DGGIST de la RCN et des représentants

des clients, il sera possible de trouver des solutions simples et réalisables à ces problèmes et à d'autres problèmes importants.

3.6 COMMUNICATIONS

3.6.1 Canaux de communications

La gestion des communications basées sur les TI suit les mêmes tendances que la gestion des autres domaines. Il y a peu de normes nationales, sinon aucune, et celles qui existent ne sont pas visibles pour les utilisateurs. En outre, sauf quelques exceptions, elles ont été élaborées sans la participation des utilisateurs/clients. Le MPO utilise tous les canaux de communications électroniques, du courrier électronique de masse jusqu'à l'Intranet, en passant par l'Internet et les dossiers publics. Il n'existe cependant aucune politique claire indiquant quel système sera utilisé pour quelle fonction et quelles communications ne se prêtent pas à la diffusion électronique. Il s'ensuit que tous les canaux sont utilisés. Bien que la gestion des éléments de TI qui sont reliés aux communications (courrier électronique de masse, Internet, Intranet et dossiers publics) soit entièrement effectuée à l'aide des TI, ces éléments représentent des approches qui, si elles étaient effectuées sur support papier (lettres à tous les employés, bulletins ministériels et régionaux, etc.), seraient entièrement gérées par la Direction générale des communications.

Nous avons relevé certaines indications de surcharge d'information chez le personnel. Un sondage réalisé en 1997, durant l'élaboration du Plan de virage écologique des opérations du Ministère, indiquait que le personnel ne trouvait pas que les messages électroniques de masse, même ceux qui étaient signés par la haute direction, étaient une façon appréciée d'obtenir de l'information. Dans la RCN, il y a eu plus de 450 envois massifs de messages électroniques en 1998, allant des offres d'emplois adressées à un groupe et à un niveau spécifiques jusqu'aux avertissements d'alarmes incendie les fins de semaine, quand très peu d'employés sont présents. Une étude officieuse réalisée dans la région du Pacifique indiquait qu'il y avait eu une moyenne de cinq envois généralisés par jour en 1998.

Il faut assurer la compatibilité, la cohérence et la qualité de l'information dans les régions et les directions générales. Compte tenu des nombreuses options possibles (Intranet, courrier électronique de masse ou dossiers publics), il est très difficile de choisir le bon moyen pour diffuser l'information. Les programmes ne savent pas quel moyen ils devraient utiliser pour communiquer. Il n'existe aucune politique, ni aucune source évidente d'orientations sur cette question. Les dossiers publics, ce qu'ils sont et comment les utiliser, sont un mystère pour la plupart des employés du Ministère. Il faut examiner le contenu des messages électroniques de masse pour voir s'il s'agit d'informations qui pourraient être transmises par d'autres moyens (comme les messages de courrier électronique portant sur le stationnement, envoyés uniquement à ceux qui utilisent le stationnement).

3.6.2 La publication Web

La gestion de la publication d'information sur l'Intranet et l'Internet se fait non seulement à la Direction générale des communications, mais aussi dans tous les secteurs de programmes du

Ministère. La publication Web est devePue une ¡ctivité°généralisée depuis l'
langage « hypertexte » qui permet de relier des documents à d'autres ressourc
comme des cartes, des tableaux et d'autres rapports. Cette activité a également
développement de moteurs de recherche « globaux » rapides, capables d'exam
d'enregistrements pour repérer un élément d'information précis. Il s'agit en f
de communications, qui mérite toutefois une attention spéciale en raison de s
surtout depuis que l'Internet a le potentiel de devenir une dépense encore plus
Industrie Canada a commencé une activité de rayonnement auprès des petites
« Strategis », dont la mise en œuvre a coûté plus de 20 millions $ et les coûts
s'établissent à plusieurs millions de dollars par année. Dans « *Technology Fo*
PriceWaterhouseCoopers indiquait qu'une présence importante sur l'Internet
plus de 10 millions $ et que les sites de commerce électronique (comme Amaz
grande librairie du monde) coûtent plus de 30 millions $ à développer et 5 mil
gérer, en raison des coûts élevés de la mise à jour de l'information. Certains
pourrait tirer avantage de dépenses pouvant atteindre 15 millions $ en publica
n'avons trouvé aucun dossier justificatif à l'appui des activités de publication

L'équipe d'examen a constaté que le MPO dépense environ 2 millions $ par a
Web, ce qui comprend les dépenses de matériels, de logiciels et les salaires. I
utilisateurs, 72 % des répondants ont indiqué qu'ils avaient utilisé l'Intranet a
précédent. L'utilité de l'information obtenue avait été cotée à environ 4 sur u
outre, 82 % des répondants ont indiqué qu'ils utilisaient l'Internet au travail.
renseignements clé à l'intention des clients (comme les rapports statistiques e
les pêches) sont maintenant disponibles uniquement sur les serveurs Web du

Il est très possible que de la documentation non contrôlée ait été et continue d
sites Web, autant pour la consommation publique sur l'Internet que pour la co
l'Intranet. Il n'existe aucun contrôle généralisé permettant de vérifier si cette
exacte et conforme aux politiques et aux mandats du MPO. La Direction gén
communications a la responsabilité d'appliquer les normes du Ministère et du
mais ses responsables ont indiqué n'exercer aucune surveillance. En fait, les p
région du Pacifique ne respectent ni les normes de présentation du Ministère,
du Trésor.
Du point de vue de l'efficacité et de l'efficience, il n'existe aucun mécanisme
vérifier si la documentation publiée sur le Web est pertinente. C'est une activ
volontaire au MPO, qui se rapporte davantage à ce qui est souhaité qu'à ce qu
nombreux groupes admettent publier sur le Web « parce c'est amusant ».
éditeurs Web ne connaissent pas vraiment leur public cible, ce qui fait qu'il e
quoi publier et quoi exclure. Même quand une étude a été faite auprès d'un gr
s'est révélé que plus de 80 % des clients participant au groupe n'avaient abso
expérience de l'Internet. Comme les outils de publication Web deviennent de
abordables et faciles à utiliser, il est probable qu'une quantité croissante d'in
diffusée pour consultation publique.

Signalons deux exceptions remarquables : la région des Maritimes et la région Laurentienne, qui ont bien planifié une bonne partie de leurs pages Web. Dans ces deux régions, on a formé des comités régionaux chargés de définir les clients et de présenter des blocs d'information mieux ciblés et plus pertinents. De telles approches constituent des « pratiques optimales » et une méthode de gestion qui devrait être mise en œuvre de façon plus générale.

3.7 FORMATION

3.7.1 Déficit de formation

D'après les résultats du sondage, la gestion des changements dans le domaine des TI semble avoir été inadéquate pour le volet formation. En effet, le sondage des utilisateurs réalisé dans le cadre de cet examen a révélé que 40 % des employés du MPO aimeraient obtenir de la formation sur les logiciels actuellement installés sur leurs ordinateurs. Le même sondage indiquait qu'environ 2 970 personnes au MPO n'avaient pas reçu de formation lors de l'installation de nouveaux logiciels et que la moitié des employés du MPO (approximativement 4 500 personnes) n'avaient pas été avisés des utilisations ou des avantages des nouveaux logiciels installés. Si l'on s'occupait de cette question, on pourrait également atténuer plusieurs problèmes reliés à la facilité d'utilisation, à la fiabilité et à la dépendance envers le Bureau d'assistance. Le personnel de la DGGIST fait état des nombreux cours offerts et des pages Intranet qui décrivent les cours disponibles, mais les résultats du sondage indiquent que ces approches n'ont pas réussi à rejoindre les 50 % des employés qui semblent toujours désirer de la formation.

Les utilisateurs d'ordinateurs veulent plus de formation qu'ils n'en ont reçue. Il s'agit probablement, en partie, d'une décision émanant des programmes, quelque peu indépendante de la DGGIST. La formation sur la suite de bureautique a été identifiée dans le sondage des utilisateurs ministériels comme un besoin par 25 % du personnel du Ministère; cependant, la DGGIST offre de la formation et les employés ont également accès à de la formation commerciale dans toutes les grandes villes. Le fait que les employés des programmes sentent le besoin de recevoir de la formation et qu'ils n'ont pas reçu de formation sur la suite de bureautique laisse croire que le personnel n'a pas demandé cette formation ou que les gestionnaires n'ont pas affecté de fonds à cette activité.

L'absence de formation sur des applications aussi répandues que la suite de bureautique a notamment pour effet que le Bureau d'assistance est inondé de demandes simples et non nécessaires. La région du Pacifique, en adoptant un Bureau d'assistance géré par du personnel interne plutôt que par un entrepreneur de l'extérieur, a indiqué qu'elle n'était pas disposée à payer un entrepreneur 37 $ l'heure pour résoudre des problèmes simples concernant l'utilisation du logiciel Word. Il existe plusieurs autres façon de résoudre ce problème, ainsi que plusieurs approches de gestion. Une première approche pourrait consister à acheminer les appels reliés aux logiciels à une organisation de service entièrement consacrée au soutien des logiciels, qui pourrait exiger des frais moins élevés que nos coûts internes. Une deuxième façon serait de limiter le nombre d'appels reliés à l'utilisation des logiciels auxquels auraient droit les utilisateurs individuels (par ex. : quatre « appels sur la suite de bureautique par personne par année »). Une troisième approche serait de contrôler la nature exacte des appels adressés au Bureau d'assistance

et de le signaler à l'un des comités utilisateurs/clients de TI pour qu'il trouve des solutions. Dans certaines organisations, on utilise un système de facturation interne basé sur les appels. Cette approche impute les coûts de formation/Bureau d'assistance directement aux gestionnaires de programmes.

À l'évidence, l'évolution de l'environnement de bureautique entraîne un besoin de formation. Chaque fois que les logiciels de base sont modifiés par l'addition de nouvelles fonctions qui affectent les utilisateurs et nécessitent de nouvelles compétences ou de la formation, les coûts et les dispositions de formation devraient être établis avant l'acquisition de nouvelles versions. Étant donné que la suite Office 97 n'est pas encore entièrement mise en œuvre, les nouvelles exigences opérationnelles associées à l'évolution de la norme nationale vers Microsoft Office 2000 (actuellement vendue en version préliminaire au grand public) devraient faire l'objet d'une étude détaillée et complète. Cela est particulièrement important, car plusieurs grandes entreprises ont décidé, en se basant sur les besoins, de continuer à utiliser Office 95 (soit la version que le MPO utilise encore sur les ordinateurs de type 486) afin d'éviter les problèmes de formation et d'incompatibilité matérielle et technique qui sont associés à Office 97. Comme il n'y a eu aucun dossier justificatif indiquant que la suite Office 97 était nécessaire aux utilisateurs du MPO pour s'acquitter de leurs responsabilités reliées aux programmes, les nombreuses difficultés matérielles et logicielles qui ont accompagné ce changement auraient pu être évitées.

Quand des logiciels spécialisés (comme le Departmental Violations System, le Habitat Referrals Tracking System, Abacus et d'autres) ont été déployés, le nombre d'employés qui ont reçu de la formation était plus élevé. Les gestionnaires considèrent peut-être les fonctions de bureau comme de la routine et reconnaissent que les applications personnalisées nécessitent de la formation spécialisée. Inversement, les gestionnaires de systèmes axés sur les programmes se sentent peut-être plus responsables de tous les aspects de la mise en œuvre, y compris la formation.

Dans la région du Pacifique, l'implantation de la suite Office 97 s'est faite de façon innovatrice. En effet, une trousse « par utilisateur » a été créée et « vendue » aux gestionnaires 125 $ par utilisateur (soit 100 $ pour une demi-journée de formation et 25 $ comme contribution au coût de la licence du logiciel et du CD-ROM). Le coût total de la licence d'exploitation de la suite Office 97 était de 78 $ par utilisateur, soit trois fois le coût facturé. La DGGIST du Pacifique avait initialement l'intention d'offrir seulement des trousses « complètes » comprenant la formation, mais elle a finalement cédé aux pressions des programmes et « vendu » des licences sans formation aux secteurs de programmes pour 25 $ l'unité. Le nouveau logiciel est donc apparu sur les bureaux du personnel des programmes sans que les utilisateurs aient été formés à son utilisation. Le sondage des utilisateurs confirme que le personnel des programmes désire toujours obtenir cette formation. La préparation d'un dossier justificatif, même dans ce cas, aurait permis de mieux gérer cette transition.

On achète souvent de nouvelles versions de logiciels de bureautique pour accéder à de nouvelles fonctions qui ne sont pas offertes dans les anciennes versions. Il est important d'évaluer, dans le cadre de comités clients-fournisseurs, si ces nouvelles fonctions sont nécessaires aux programmes. En outre, la formation nécessaire à l'utilisation de ces fonctions doit être prise en compte dans les coûts et les avantages. Dans l'exemple mentionné ci-dessus, si l'on considère le prix de 100 $ par

utilisateur utilisé par la région du Pacifique comme un coût de formation raisonnable pour le Ministère, la licence d'Office 97 a elle-même coûté 700 000 $. Cependant, elle a créé, pour les programmes, un besoin de formation de 900 000 $ (9 000 employés à 100 $ chacun), ce qui a porté le coût réel (non relié aux matériels) à 1,6 millions $. Lors de toutes les mises à niveaux futures, les coûts de formation devront être compris dans le dossier justificatif présenté à l'appui du changement. La formation doit faire partie de tout changement apporté au système et la formation sur les versions existantes et nouvelles du logiciel de courrier électronique et de la suite de bureautique devrait être considérée faire partie des coûts de réseau.

Certains prétendent qu'il arrive souvent que les changements coûteux, même s'ils ne sont pas nécessaires aux utilisateurs, facilitent souvent les fonctions de la DGGIST. Cela ne diminue pas la nécessité d'une analyse complète des avantages et des coûts (y compris le dérangement, la formation et le nouveau matériel) qui accompagneraient de tels changements. Certes, Microsoft offre aux gestionnaires de TI des séminaires gratuits sur la suite Office 2000 en annonçant que ce produit est plus facile et moins coûteux à gérer qu'Office 97, mais en ne disant rien sur les exigences de nouveaux matériels ni sur les questions d'interopérabilité. Comme nous l'avons indiqué ailleurs dans ce rapport, un dossier justificatif analytique, envisageant les produits d'une variété de fabricants, devrait précéder ce type d'investissement.

Enfin, le sondage des utilisateurs indiquait qu'entre 12 % et 28 % des employés ministériels ont « renoncé » à résoudre des problèmes informatiques ayant négativement affecté ou limité leur capacité à s'acquitter de leurs responsabilités de travail. Cette proportion aurait probablement été moindre si la formation demandée (40 % du personnel) avait été fournie.

4.0 RECOMMANDATIONS

Nous recommandons

4.1 Que le Ministère mette rapidement en place un processus décisionnel qui fasse en sorte que les investissements de TI soient entièrement évalués, à la fois sur le plan de leur soutien des besoins des programmes ministériels et sur le plan de leur conformité aux normes et à l'architecture ministérielles. Un tel système devrait préciser les responsabilités afférentes à la gestion de tous les actifs, services, normes et architecture de TI. Ce processus doit faire appel à la participation du personnel et des clients de la DGGIST, dans toutes les régions et la RCN. Le processus qui a été suivi pour l'élaboration du document sur l'architecture informatique est un bon modèle.

4.2 Que le Ministère s'assure que les grands systèmes de TI sont évalués au moyen d'un outil complet d'évaluation et de planification de projet. Les Maritimes et la région Laurentienne utilisent un système qui a été conçu pour le MPO et qui s'est révélé utile pour assurer la mise en œuvre harmonieuse des grands systèmes.

4.3 Que le Ministère établisse un financement fiable et à long terme pour les éléments de TI qui sont fondamentaux aux communications et à l'interopérabilité, ce qui comprend les télécommunications, les matériels et les logiciels qui soutiennent le RE et les RL, ainsi que

la suite de bureautique standard et le système de courrier électronique. Le financement du personnel responsable de l'exploitation et de la maintenance de ce système (soit directement, soit sous contrat) ainsi que du personnel du Bureau d'assistance et des gestionnaires de portefeuilles devrait être inclus. Le niveau de financement continu devrait reconnaître l'évolution rapide qui est caractéristique des TI, tout en mettant l'accent sur ce qui est nécessaire au MPO pour s'acquitter de ses responsabilités de programmes.

4.4 Que la DGGIST des Services intégrés réalise une évaluation de la menace et des risques visant le réseau, en accordant la priorité à l'évaluation des menaces posées par l'actuelle architecture de l'accès Internet au MPO afin d'établir s'il s'agit d'un niveau de risque acceptable.

4.5 Que les responsables de la DGGIST des Services intégrés dans les régions et la RCN travaillent en collaboration pour identifier les produits et les services, y compris les rapports, les temps de réponse acceptables et les niveaux de services, qui sont nécessaires au fonctionnement du RE. Cette identification devrait être utilisée pour obtenir, par appel d'offres, des services d'évaluation et de rapports sur les télécommunications et le réseau pour les exercices subséquents. En outre, il faudrait réaliser une évaluation complète des produits, des services et des niveaux de services qui auraient dû être fournis par les SGTI dans le cadre du présent contrat, mais qui ne l'ont pas été. Si le déficit de services identifié par cette analyse se révèle substantiel, des mesures correctives devraient être prises.

4.6 Que la DGGIST des Services intégrés prenne des mesures pour aviser les utilisateurs de la sécurité des systèmes électroniques actuels du MPO, et de la mesure dans laquelle ces systèmes devraient être utilisés pour traiter ou transmettre de l'information sensible. Il faudrait réaliser une évaluation pour déterminer dans quelle mesure le MPO a besoin du chiffrement et de l'authentification sécurisée pour le courrier électronique et les transactions financières.

4.7 Que la DGGIST des Services intégrés élabore, en collaboration avec le personnel des programmes et des ressources humaines, un mécanisme pour corriger le « déficit de formation » identifié dans le cadre de cet examen. Plus de la moitié de ce déficit est reliée à l'exploitation de la suite de bureautique actuelle.

4.8 Que les membres de la DGGIST des Services intégrés dans les régions et la RCN collaborent avec les clients pour établir des moyens raisonnables et efficaces de normaliser :

4.8.1 Les niveaux acceptables de performance du réseau
4.8.2 Les règles régissant les systèmes coupe-feu
4.8.3 Les niveaux de services à l'intention des petits bureaux, des sites éloignés et des navires
4.8.4 Un mécanisme permettant d'évaluer l'évolution de la norme de bureautique et du système de courrier électronique

4.8.5 Une suite d'énoncés de politiques dans les domaines identifiés à la section 3.4.1 de ce rapport
4.8.6 Les services et les domaines devant faire l'objet d'un soutien permanent (24 heures sur 24)
4.8.7 Les services et les domaines qui ne doivent avoir aucun point de défaillance
4.8.8 Les dispositions de facturation interne et de soutien pour les grandes initiatives multi-régionales de TI basées sur les programmes
4.8.9 Les services de TI et de RE/RL devant être fournis aux ministères locataires (comme RNCan)

4.9 Que la DGGIST des Services intégrés élabore une définition complète des besoins pour le RE, comprenant des critères de performance clairement établis, des exigences de rapports basées sur les besoins du personnel de la DGGIST dans la RCN et dans les régions, et des pénalités pour inexécution des normes spécifiées, et utilise ces exigences et critères comme base d'attribution du contrat de services pour le RE afin d'éviter les nombreuses faiblesses identifiées dans les dispositions actuellement en vigueur.

4.10 Que les mesures prises par le personnel régional de la DGGIST des Services intégrés pour résoudre les incohérences de l'architecture et des systèmes coupe-feu soient élargies pour englober le personnel et les clients de la RCN afin qu'une solution complète tenant compte des besoins des clients puisse être mise en œuvre.

4.11 Que la DGGIST des Services intégrés et la Direction générale des communications collaborent pour identifier une approche ordonnée et raisonnable pour l'utilisation des communications électroniques et le partage de l'information. Les consultations devraient inclure les secteurs de programmes qui ont actuellement recours à la publication Web interne et sur l'Internet.

4.12 Que la Garde côtière canadienne, en collaboration avec les SGTI et la DGGIST des Services intégrés, évalue dans quelle mesure il est possible de répondre aux besoins des programmes et de réaliser des économies en harmonisant l'acquisition des services de télécommunications. Cette évaluation est particulièrement souhaitable en raison des similarités techniques du système INNAV qui sera bientôt mis en œuvre et des équipements et liaisons actuellement exploités par la DGGIST des Services intégrés.

4.13 Que la DGGIST des Services intégrés élabore et diffuse une politique d'utilisation acceptable des ressources de TI pour préciser ce qui est acceptable, et ce qui ne l'est pas, à l'intention des employés du MPO.

REMERCIEMENTS

Nous remercions tout spécialement le personnel de la DGGIST des Services intégrés dans la RCN et dans toutes les régions. Nous tenons également à remercier le Directeur général de la DGGIST qui, tout au long de cet exercice, a pris toutes les mesures nécessaires pour que l'équipe d'examen

obtienne toute l'information qui lui était nécessaire. En outre, plusieurs directeurs et de nombreux employés des sections technique et soutien de la fonction informatique ont pris le temps de nous faire des observations utiles, d'examiner nos conclusions préliminaires et de nous expliquer les particularités d'un système complexe.

5.0. PLAN D'ACTION DE LA DIRECTION

Contexte de l'examen

Pêches et Océans a un éventail complexe de missions, dont bon nombre d'aspects essentiels dépendent de la technologie de l'information. En raison de cette dépendance et de l'étendue géographique du Ministère, le MPO a investi tôt et continuellement dans la technologie de l'information.

Les scientifiques du Ministère ont commencé à utiliser les ordinateurs dés le tout début de leur existence. On leur doit certainement aussi des innovations essentielles qui ont été mises au point pour rassembler et analyser au moyen de l'informatique de grandes quantités de renseignements. En outre, c'est la communauté scientifique qui a été à l'origine de la création de l'Internet. Les employés des Sciences du MPO utilisent l'Internet pour communiquer et collaborer avec des scientifiques des quatre coins du monde depuis qu'il est possible de le faire. Aussi, une bonne partie des renseignements qui sont transmis aux clients et à la communauté universitaire le sont grâce à la technologie de l'information.

La Garde côtière canadienne, en raison de ses responsabilités liées à la navigation et à la recherche et sauvetage, s'est placée, elle aussi, à l'avant-garde comme utilisatrice de la technologie de l'information. Les renseignements sur la navigation et sur la sécurité proviennent de partout, d'un bout à l'autre du pays, depuis des phares isolés jusqu'à des ports achalandés.

Le MPO a toujours été un précurseur dans l'adoption des nouveaux modes de communication, d'analyse et d'exécution fondés sur la technologie de l'information. La mise en service de systèmes électroniques nationaux pour le courrier, les finances et les ressources humaines en est la preuve. Le sondage mené dans le cadre de l'examen a révélé que pratiquement tous les répondants (97,4 %) disent avoir accès à un ordinateur ou se servir d'un ordinateur pour accomplir leurs tâches quotidiennes. L'accès à des ordinateurs à l'échelle du Ministère semble uniforme, car au moins 90 % des répondants de toutes les régions et de tous les secteurs ont indiqué qu'ils utilisent un ordinateur pour s'acquitter de leurs tâches habituelles.

Le MPO a fait des investissements importants dans la technologie de l'information et continue de le faire. À l'époque où l'examen a été mené, le MPO dépensait 6 650 $ par employé chaque année pour la technologie de l'information. L'examen a identifié des domaines d'intervention importants et présenté des recommandations en ce qui les concerne. La mise en œuvre des recommandations de ce rapport entraînera une utilisation meilleure et plus rentable de la technologie de l'information.

5.0. PLAN D'ACTION DE GESTION

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
1. Que le Ministère mette rapidement en place un processus décisionnel qui fasse en sorte que les investissements de TI soient entièrement évalués, à la fois sur le plan de leur soutien des besoins des programmes ministériels et sur le plan de leur conformité aux normes et à l'architecture ministérielles. Un tel système devrait préciser les responsabilités afférentes à la gestion de tous les actifs, services, normes et architecture de TI. Ce processus doit faire appel à la participation du personnel et des clients de la DGGIST, dans toutes les régions et la RCN. Le processus qui a été suivi pour l'élaboration du document sur l'architecture informatique est un bon modèle.	Le CDI a été formé et a recommandé l'adoption d'un processus ministériel d'examen des projets en informatique. Ce processus comprendra un examen ministériel des projets qui visent à réduire les risques, à évaluer les conditions de réussite, à réduire le dédoublement et à optimiser les résultats en conformité des orientations stratégiques et activités prioritaires du MPO. Notre stratégie consiste à mettre en œuvre le processus d'approbation pour les initiatives liées à des systèmes de grande envergure, à montrer la validité et l'utilité de ce processus et ensuite à mettre en œuvre des processus semblables (à d'autres niveaux et peut-être à plus petite échelle) pour des initiatives de moindre envergure. Entre-temps, le modèle est en train d'être évalué pour l'utilisation dans plusieurs régions et secteurs.	Directeur, Direction des services de planification et de gestion de l'information	1er septembre 2000
2. Que le Ministère s'assure que les grands systèmes de TI sont évalués au moyen d'un outil complet d'évaluation et de planification de projet. Les Maritimes et la région Laurentienne utilisent un système	Pour les grands projets de TI, la Direction des services d'applications (DSA) encouragera l'utilisation de deux ensembles de compétences pour la gestion de projets : *Planification de projet logiciel* et *Suivi et supervision de projet logiciel*. Ces processus de gestion des projets font partie	Directeur, Direction des services d'applications	La formation et les séances de la DSA ont commencé. Recommandation pour la trousse

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
qui a été conçu pour le MPO et qui s'est révélé utile pour assurer la mise en œuvre harmonieuse des grands systèmes.	intégrante du Cadre amélioré de gestion (CAG) du Conseil du Trésor. La DSA en fera la promotion par le truchement de séances qui auront lieu dans la RCN et dans les régions, au cours desquelles le CAG servira de cadre de travail. Les employés de la DSA sont en train de recevoir de la formation pour les deux ensembles de compétences et sont encouragés à obtenir l'accréditation pour la gestion de projets. Des outils de gestion des projets sont aussi en train d'être évalués. Nous proposerons au CGM/CEM une trousse d'outils standard pour la gestion des projets.		d'outils : au plus tard en juin 2000.
3. Que le Ministère établisse un financement fiable et à long terme pour les éléments de TI qui sont fondamentaux aux communications et à l'interopérabilité, ce qui comprend les télécommunications, les matériels et les logiciels qui soutiennent le RE et les RL, ainsi que la suite de bureautique standard et le système de courrier électronique. Le financement du personnel responsable de l'exploitation et de la maintenance de ce système (soit directement, soit sous contrat) ainsi que du personnel	➢ Présenter au CDI/CGM une analyse des options et une recommandation au sujet de la décision concernant les besoins en financement courants liés à l'actif pour l'infrastructure d'informatique partagée du MPO afin d'offrir des niveaux de services uniformes et raisonnables à l'échelle du Ministère. ➢ Présenter au CGM, pour approbation de financement, les besoins liés à la remise à neuf des immobilisations pour l'infrastructure	DG, GIST Directeur, Services de planification et de gestion de	Janvier 2000 – l'actif a été examiné, et nous sommes en train d'élaborer une stratégie de recouvrement des coûts pour l'informatique à l'échelle du MPO. Date cible : juin 2000 Automne 1999 – les besoins ont été présentés. Le

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
du Bureau d'assistance et des gestionnaires de portefeuilles devrait être inclus. Le niveau de financement continu devrait reconnaître l'évolution rapide qui est caractéristique des TI, tout en mettant l'accent sur ce qui est nécessaire au MPO pour s'acquitter de ses responsabilités de programmes.	informatique partagée, conformément au PILT. ➢ S'assurer que les organisations régionales de la DGGIST participent pleinement au processus de planification des activités du MPO ainsi qu'aux processus d'identification de l'actif, de la remise à neuf, d'investissement et de planification liés au PILT.	l'information Directeur, Services de planification et de gestion de l'information	PILT n'est pas encore définitif ni approuvé. Automne 1999 – toutes les organisations ont participé
4. Que la DGGIST des Services intégrés réalise une évaluation de la menace et des risques visant le réseau, en accordant la priorité à l'évaluation des menaces posées par l'actuelle architecture de l'accès Internet au MPO afin d'établir s'il s'agit d'un niveau de risque acceptable.	La DGGIST des Services intégrés mènera une évaluation complète de la menace et des risques en ce qui concerne l'infrastructure nationale, notamment la structure de l'emplacement et des politiques de tous les systèmes coupe-feu ainsi que l'architecture du système du courrier électronique, au plus tard le 1er septembre 2000.	Directeur, Services de la technologie	1er septembre 2000
5. Que les responsables de la DGGIST des Services intégrés dans les régions et la RCN travaillent en collaboration pour identifier les produits et les services, y compris les rapports, les temps de réponse acceptables et les niveaux de	Les responsables de la DGGIST des Services intégrés dans les régions et dans la RCN identifieront les produits et les services nécessaires au fonctionnement du RE, y compris les rapports, les temps de réponse acceptables et les niveaux de services.	Directeur, Services de la technologie	1er septembre 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
services, qui sont nécessaires au fonctionnement du RE. Cette identification devrait être utilisée pour obtenir, par appel d'offres, des services d'évaluation et de rapports sur les télécommunications et le réseau pour les exercices subséquents. En outre, il faudrait réaliser une évaluation complète des produits, des services et des niveaux de services qui auraient dû être fournis par les SGTI dans le cadre du présent contrat, mais qui ne l'ont pas été. Si le déficit de services identifié par cette analyse se révèle substantiel, des mesures correctives devraient être prises.			
6. Que la DGGIST des Services intégrés prenne des mesures pour aviser les utilisateurs de la sécurité des systèmes électroniques actuels du MPO, et de la mesure dans laquelle ces systèmes devraient être utilisés pour traiter ou transmettre de l'information sensible. Il faudrait réaliser une évaluation pour déterminer dans quelle mesure le	Chaque trimestre, les responsables de la DGGIST des Services intégrés enverront un message à tous les utilisateurs du courrier électronique pour leur rappeler que les renseignements protégés ou de nature délicate ne doivent pas être transmis par courrier électronique.	Directeur, Services de la technologie	À partir du 1er septembre 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
MPO a besoin du chiffrement et de l'authentification sécurisée pour le courrier électronique et les transactions financières.			
7. Que la DGGIST des Services intégrés élabore, en collaboration avec le personnel des programmes et des ressources humaines, un mécanisme pour corriger le « déficit de formation » identifié dans le cadre de cet examen. Plus de la moitié de ce déficit est reliée à l'exploitation de la suite de bureautique actuelle.	Des comités d'utilisateurs régionaux examineront le déficit de formation des « utilisateurs finals » et établiront des estimations de coûts ainsi qu'un plan d'action, en collaboration avec les représentants de la DGGIST et des RH. Les Services intégrés entament actuellement la mise en œuvre d'une initiative « d'organisation apprenante ». Nous nous assurerons que nos partenaires s'en occupent et nous présenterons des recommandations au CGM.	Directeurs régionaux de l'informatique (toutes les régions)	Ébauche du plan d'action : au plus tard le 31 mars 2000 31 mars 2000
8. Que les membres de la DGGIST des Services intégrés dans les régions et la RCN collaborent avec les clients pour établir des moyens raisonnables et efficaces de normaliser : 1) Les niveaux acceptables de performance du réseau 2) Les règles régissant les systèmes coupe-feu 3) Les niveaux de services à l'intention des petits bureaux, des sites éloignés et des navires	Les membres de la DGGIST des Services intégrés élaboreront un plan de travail correspondant à chaque enjeu et présenteront un plan d'action en plus[illegible]s points pour chacun de ces enjeux au Comité national de l'informatique, au plus tard le 1er septembre 2000.	Directeur, Services de la technologie	1er septembre 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
4) Un mécanisme permettant d'évaluer l'évolution de la norme de bureautique et du système de courrier électronique 5) Une suite d'énoncés de politiques dans les domaines identifiés à la section 3.4.1 de ce rapport 6) Les services et les domaines devant faire l'objet d'un soutien permanent (24 heures sur 24) 7) Les services et les domaines qui ne doivent avoir aucun point de défaillance 8) Les dispositions de facturation interne et de soutien pour les grandes initiatives multi-régionales de TI basées sur les programmes 9) Les services de TI et de RE/RL devant être fournis aux ministères locataires (comme RNCan)			
9. Que la DGGIST des Services intégrés élabore une définition complète des besoins pour le RE, comprenant des critères de performance clairement établis, des	Des services de télécommunications seront acquis afin d'atteindre des objectifs précisés concernant le rendement et la sécurité.	Directeur, Services de la technologie	Début : 1er avril 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
exigences de rapports basées sur les besoins du personnel de la DGGIST dans la RCN et dans les régions, et des pénalités pour inexécution des normes spécifiées, et utilise ces exigences et critères comme base d'attribution du contrat de services pour le RE afin d'éviter les nombreuses faiblesses identifiées dans les dispositions actuellement en vigueur.			
10. Que les mesures prises par le personnel régional de la DGGIST des Services intégrés pour résoudre les incohérences de l'architecture et des systèmes coupe-feu soient élargies pour englober le personnel et les clients de la RCN afin qu'une solution complète tenant compte des besoins des clients puisse être mise en œuvre.	Mettre en œuvre et raffiner le plan actuel de remplacement et de gestion des systèmes coupe-feu et travailler de concert avec les clients, dans le cadre de la gestion et de la maintenance courantes de l'infrastructure.	Directeur, Services de la technologie	1er septembre 2000
11. Que la DGGIST des Services intégrés et la Direction générale des communications collaborent pour identifier une approche ordonnée et	La DGGIST des Services intégrés travaillera en collaboration avec les Communications du MPO afin d'élaborer un plan détaillé regroupant les activités du MPO liées au Web et assurant l'adoption	Directeur, Services de planification et de gestion de l'information	1er avril 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
raisonnable pour l'utilisation des communications électroniques et le partage de l'information. Les consultations devraient inclure les secteurs de programmes qui ont actuellement recours à la publication Web interne et sur l'Internet..	d'approches systématiques et normalisées de même que l'élimination de l'information désuète et non pertinente.	/ Directeur Direction des opérations, Communications	
12. Que la Garde côtière canadienne, en collaboration avec les SGTI et la DGGIST des Services intégrés, évalue dans quelle mesure il est possible de répondre aux besoins des programmes et de réaliser des économies en harmonisant l'acquisition des services de télécommunications. Cette évaluation est particulièrement souhaitable en raison des similarités techniques du système INMAV qui sera bientôt mis en œuvre et des équipements et liaisons actuellement	La DGGIST des Services intégrés, en collaboration avec la Garde côtière, identifiera les domaines pour lesquels l'acquisition harmonisée de services de télécommunications serait avantageuse. Un compte rendu de ces discussions sera déposé au Comité national de l'informatique, au plus tard le 1er septembre 2000.	Directeur, Services de la technologie / DG, Services techniques et opérationnels - GCC	1er avril 2000

RECOMMANDATIONS	PLAN D'ACTION DE LA DIRECTION	AGENT DE PREMIÈRE RESPONSABILITÉ	DATE CIBLE INITIALE
ressources de TI pour préciser ce qui est acceptable, et ce qui ne l'est pas, à l'intention des employés du MPO.	Conseil du Trésor, et en fera rapport au Comité national de l'informatique tous les trois mois. La DGGIST s'assurera aussi que des mesures sont prises dans les cas d'utilisation inacceptable.	l'information	